Εγχειρίδιο του FreeBSD

Περίληψη

Καλώς ήρθατε στο FreeBSD! Αυτό το εγχειρίδιο καλύπτει την εγκατάσταση και την καθημερινή χρήση του *FreeBSD 11.2-RELEASE* και του *FreeBSD 12.0-RELEASE*. Το βιβλίο αυτό είναι *μόνιμα υπό βελτίωση και ανάπτυξη* και αποτελεί το αποτέλεσμα της δουλειάς πολλών ατόμων, οπότε κάποια τμήματα μπορεί να περιέχουν σχετικά ξεπερασμένες πληροφορίες και να χρειάζονται ανανέωση. Αν ενδιαφέρεστε να μας βοηθήσετε σε αυτό το έργο, επικοινωνήστε μαζί μας στην ηλεκτρονική λίστα ομάδας τεκμηρίωσης του FreeBSD. Η τελευταία έκδοση αυτού του κειμένου είναι πάντα διαθέσιμη από την ιστοσελίδα του FreeBSD (παλιότερες εκδόσεις μπορείτε να βρείτε στη διεύθυνση http://docs.FreeBSD.org/doc/). Μπορείτε επίσης να μεταφορτώσετε στον υπολογιστή σας το ίδιο βιβλίο σε άλλες μορφές αρχείου και με διάφορες μορφές συμπίεσης από τον εξυπηρετητή FTP του FreeBSD ή ένα από τα πολλά mirror sites. Αν προτιμάτε ένα τυπωμένο αντίτυπο, μπορείτε να αγοράσετε ένα αντίγραφο του Εγχειριδίου, από το FreeBSD Mall. Μπορείτε επίσης να ψάξετε σε όλο το βιβλίο.

Πίνακας Περιεχομένων

Πρόλογος . . . 13
Σε Ποιους Απευθύνεται Αυτό το Βιβλίο . . . 13
Αλλαγές από την Τρίτη Έκδοση . . . 13
Αλλαγές από τη Δεύτερη Έκδοση (2004) . . . 13
Αλλαγές από την Πρώτη Έκδοση (2001) . . . 14
Οργάνωση Αυτού του Βιβλίου . . . 15
Συμβάσεις που χρησιμοποιούνται σε αυτό το βιβλίο . . . 19
Ευχαριστίες . . . 20
I: Εισαγωγή . . . 21
1. Σύνοψη . . . 22
2. Καλώς ήλθατε στο FreeBSD! . . . 23
2.1. Τι μπορεί να κάνει το FreeBSD; . . . 23
2.2. Ποιος χρησιμοποιεί FreeBSD; . . . 25
3. Πληροφορίες για το FreeBSD Project . . . 29
3.1. Μια σύντομη ιστορία του FreeBSD . . . 29
3.2. Στόχοι του FreeBSD Project . . . 30
3.3. Το Μοντέλο Ανάπτυξης του FreeBSD . . . 30
3.4. Προγράμματα Τρίτων Κατασκευαστών . . . 32
3.5. Πρόσθετη Τεκμηρίωση . . . 32
4. Εγκατάσταση του FreeBSD 9.x και Μεταγενέστερων Εκδόσεων . . . 34
4.1. Σύνοψη . . . 34
4.2. Απαιτήσεις Υλικού . . . 34
4.3. Εργασίες πριν την Εγκατάσταση . . . 35
4.4. Ξεκινώντας την Εγκατάσταση . . . 40
4.5. Εισαγωγή στο bsdinstall . . . 44
4.6. Εγκατάσταση από το Δίκτυο . . . 48
4.7. Εκχώρηση Χώρου στο Δίσκο . . . 49
4.8. Επιβεβαίωση της Εγκατάστασης . . . 55
4.9. Μετά την Εγκατάσταση . . . 58
4.10. Αντιμετώπιση Προβλημάτων . . . 82
4.11. Χρησιμοποιώντας τη Λειτουργία Live CD . . . 83
5. Βασικές Έννοιες στο UNIX® . . . 84
5.1. Σύνοψη . . . 84
5.2. Εικονικές Κονσόλες και Τερματικά . . . 84
5.3. Άδειες (Permissions) . . . 88
5.4. Δομή Καταλόγου . . . 94
5.5. Οργάνωση Δίσκου . . . 97
5.6. Προσάρτηση και Αποπροσάρτηση Συστημάτων Αρχείων . . . 103

5.7. Διεργασίες . . . 106
5.8. Δαίμονες, Σήματα, και Τερματισμός Διεργασιών . . . 108
5.9. Κελύφη . . . 111
5.10. Κειμενογράφοι . . . 113
5.11. Συσκευές και Αρχεία συσκευών . . . 114
5.12. Τύποι Εκτελέσιμων . . . 114
5.13. Για Περισσότερες Πληροφορίες . . . 116
6. Εγκατάσταση Εφαρμογών: Πακέτα και Ports . . . 119
6.1. Σύνοψη . . . 119
6.2. Επισκόπησή της εγκατάστασης λογισμικού . . . 119
6.3. Βρίσκοντας την Εφαρμογή σας . . . 121
6.4. Χρησιμοποιώντας το Σύστημα των Πακέτων . . . 123
6.5. Χρησιμοποιώντας την Συλλογή των Ports . . . 126
6.6. Ενέργειες μετά την Εγκατάσταση . . . 137
6.7. Αντιμετωπίζοντας Χαλασμένα Ports . . . 138
7. Το Σύστημα X Window . . . 140
7.1. Σύνοψη . . . 140
7.2. Κατανόηση του περιβάλλοντος X11 . . . 140
7.3. Εγκατάσταση του X11 . . . 143
7.4. Ρύθμιση του X11 . . . 144
7.5. Χρήση Γραμματοσειρών στο X11 . . . 151
7.6. Ο X Display Manager . . . 155
7.7. Γραφικά Περιβάλλοντα . . . 158
II: Desktop Εφαρμογές . . . 164
8. Σύνοψη . . . 165
9. Φυλλομετρητές (Browsers) . . . 166
9.1. Firefox . . . 166
9.2. Opera . . . 167
9.3. Konqueror . . . 168
9.4. Chromium . . . 168
9.5. Ο Chromium και το Πρόσθετο της Java™ . . . 169
9.6. Ο Chromium και το Πρόσθετο Adobe® Flash™ . . . 169
10. Εφαρμογές Γραφείου . . . 170
10.1. KOffice . . . 170
10.2. AbiWord . . . 170
10.3. Το GIMP . . . 171
10.4. OpenOffice.org . . . 171
10.5. LibreOffice . . . 173
11. Προγράμματα Προβολής Εγγράφων . . . 175
11.1. Acrobat Reader® . . . 175
11.2. gv . . . 175

11.3. Xpdf . . . 176
11.4. GQview . . . 176
12. Χρηματοοικονομικές Εφαρμογές . . . 177
12.1. GnuCash . . . 177
12.2. Gnumeric . . . 177
12.3. Abacus . . . 178
12.4. KMyMoney . . . 178
13. Περίληψη . . . 180
14. Πολυμέσα . . . 181
14.1. Σύνοψη . . . 181
14.2. Ρύθμιση της Κάρτας Ήχου . . . 182
14.3. Ήχος MP3 . . . 187
14.4. Αναπαραγωγή Video . . . 190
14.5. Ρύθμιση Κάρτας Τηλεόρασης . . . 199
14.6. MythTV . . . 201
14.7. Σαρωτές Εικόνας . . . 202
15. Ρυθμίζοντας τον Πυρήνα του FreeBSD . . . 209
15.1. Σύνοψη . . . 209
15.2. Γιατί να Φτιάξετε Προσαρμοσμένο Πυρήνα; . . . 209
15.3. Ανακαλύπτοντας τις Συσκευές του Συστήματος σας . . . 210
15.4. Προγράμματα Οδήγησης, Υποσυστήματα και Αρθρώματα (modules) . . . 211
15.5. Δημιουργία και Εγκατάσταση Προσαρμοσμένου Πυρήνα . . . 212
15.6. Το Αρχείο Ρυθμίσεων . . . 215
15.7. Αν Κάτι Πάει Λάθος . . . 233
16. Εκτυπώσεις . . . 235
16.1. Σύνοψη . . . 235
16.2. Εισαγωγή . . . 235
16.3. Βασική Εγκατάσταση . . . 237
16.4. Ρυθμίσεις Εκτυπωτών για Προχωρημένους . . . 252
16.5. Χρήση Εκτυπωτών . . . 286
16.6. Εναλλακτικές Λύσεις για τον Στάνταρ Spooler . . . 294
16.7. Εντοπισμός Βλαβών . . . 295
17. Συμβατότητα με Εκτελέσιμα του Linux . . . 299
17.1. Σύνοψη . . . 299
17.2. Εγκατάσταση . . . 299
17.3. Εγκαθιστώντας το Mathematica® . . . 303
17.4. Εγκαθιστώντας το Maple™ . . . 306
17.5. Εγκαθιστώντας το MATLAB® . . . 308
17.6. Εγκατάσταση της Oracle® . . . 311
17.7. Προχωρημένα Θέματα . . . 315
III: Ρύθμιση και Βελτιστοποίηση . . . 318

18. Σύνοψη . . . 319
19. Αρχική Ρύθμιση . . . 320
19.1. Διάταξη Κατατμήσεων . . . 320
20. Κύρια Ρύθμιση . . . 322
21. Ρύθμιση Εφαρμογών . . . 323
22. Εκκινώντας Υπηρεσίες . . . 324
22.1. Εκτεταμένη Ρύθμιση Εφαρμογών . . . 325
22.2. Χρησιμοποιώντας Υπηρεσίες Για Την Εκκίνηση Υπηρεσιών . . . 326
23. Ρυθμίζοντας Το Πρόγραμμα cron . . . 327
23.1. Εγκαθιστώντας Ένα Crontab . . . 328
24. Χρησιμοποιώντας Το Σύστημα rc Στο FreeBSD . . . 330
25. Ρυθμίζοντας Τις Κάρτες Δικτύου . . . 332
25.1. Εντοπίζοντας Τον Σωστό Οδηγό . . . 332
25.2. Ρυθμίζοντας Την Κάρτα Δικτύου . . . 334
25.3. Δοκιμές Και Επίλυση Προβλημάτων . . . 336
26. Εικονικά Hosts . . . 339
27. Αρχεία Ρυθμίσεων . . . 340
27.1. Ο κατάλογος /etc . . . 340
27.2. Hostnames . . . 340
27.3. Log File Configuration . . . 342
27.4. sysctl.conf . . . 343
28. Tuning with sysctl . . . 345
28.1. sysctl(8) Read-only . . . 345
29. Tuning Disks . . . 347
29.1. Sysctl Variables . . . 347
29.2. Soft Updates . . . 348
30. Tuning Kernel Limits . . . 351
30.1. File/Process Limits . . . 351
30.2. Network Limits . . . 352
30.3. Virtual Memory . . . 353
31. Adding Swap Space . . . 355
31.1. Swap on a New Hard Drive . . . 355
31.2. Swapping over NFS . . . 355
31.3. Swapfiles . . . 355
32. Power and Resource Management . . . 357
32.1. What Is ACPI? . . . 357
32.2. Shortcomings of Advanced Power Management (APM) . . . 357
32.3. Configuring ACPI . . . 358
33. Using and Debugging FreeBSD ACPI . . . 359
33.1. Submitting Debugging Information . . . 359
33.2. Background . . . 360

33.3. Common Problems . . . 360
33.4. ASL, acpidump, and IASL . . . 362
33.5. Fixing Your ASL . . . 363
33.6. Getting Debugging Output From ACPI . . . 364
33.7. References . . . 364
34. Η Διαδικασία Εκκίνησης του FreeBSD . . . 365
34.1. Σύνοψη . . . 365
34.2. Το Πρόβλημα της Εκκίνησης . . . 365
34.3. Ο Διαχειριστής Εκκίνησης και τα Στάδια Εκκίνησης . . . 366
34.4. Αλληλεπίδραση με τον Πυρήνα κατά την Εκκίνηση . . . 374
34.5. Device Hints . . . 374
34.6. Init: Αρχικοποίηση Ελέγχου Διαδικασιών . . . 375
34.7. Ακολουθία Τερματισμού . . . 376
35. Ασφάλεια . . . 378
35.1. Σύνοψη . . . 378
35.2. Introduction . . . 379
35.3. Securing FreeBSD . . . 380
35.4. DES, MD5, and Crypt . . . 387
35.5. One-time Passwords . . . 388
35.6. TCP Wrappers . . . 392
35.7. KerberosIV . . . 395
35.8. Kerberos5 . . . 403
35.9. OpenSSL . . . 411
35.10. VPN over IPsec . . . 414
35.11. OpenSSH . . . 426
35.12. File System Access Control Lists . . . 432
35.13. Monitoring Third Party Security Issues . . . 434
35.14. FreeBSD Security Advisories . . . 435
35.15. Process Accounting . . . 437
36. Jails . . . 439
36.1. Σύνοψη . . . 439
36.2. Όροι των Jails . . . 439
36.3. Εισαγωγή . . . 440
36.4. Δημιουργώντας και Ελέγχοντας Jails . . . 441
36.5. Λεπτομερής Ρύθμιση και Διαχείριση . . . 443
36.6. Εφαρμογή των Jails . . . 445
37. Υποχρεωτικός Έλεγχος Πρόσβασης . . . 452
37.1. Σύνοψη . . . 452
37.2. Key Terms in this Chapter . . . 453
37.3. Explanation of MAC . . . 454
37.4. Understanding MAC Labels . . . 456

37.5. Planning the Security Configuration . . . 460
37.6. Module Configuration . . . 461
37.7. The MAC bsdextended Module . . . 462
37.8. The MAC ifoff Module . . . 463
37.9. The MAC portacl Module . . . 464
37.10. The MAC partition Module . . . 465
37.11. The MAC Multi-Level Security Module . . . 466
37.12. The MAC Biba Module . . . 468
37.13. The MAC LOMAC Module . . . 470
37.14. Nagios in a MAC Jail . . . 470
37.15. User Lock Down . . . 474
37.16. Troubleshooting the MAC Framework . . . 475
38. Έλεγχος Συμβάντων Ασφαλείας . . . 477
38.1. Σύνοψη . . . 477
38.2. Key Terms in this Chapter . . . 478
38.3. Installing Audit Support . . . 478
38.4. Audit Configuration . . . 479
38.5. Administering the Audit Subsystem . . . 482
39. Αποθηκευτικά Μέσα . . . 485
39.1. Σύνοψη . . . 485
39.2. Device Names . . . 485
39.3. Adding Disks . . . 486
39.4. USB Storage Devices . . . 487
39.5. Creating and Using CD Media . . . 489
39.6. Creating and Using DVD Media . . . 496
39.7. Creating and Using Floppy Disks . . . 501
39.8. Creating and Using Data Tapes . . . 503
39.9. Backup Strategies . . . 504
39.10. Backup Basics . . . 505
39.11. Network, Memory, and File-Backed File Systems . . . 509
39.12. File System Snapshots . . . 511
39.13. File System Quotas . . . 512
39.14. Encrypting Disk Partitions . . . 516
39.15. Encrypting Swap Space . . . 523
39.16. Highly Available Storage (HAST) . . . 524
40. GEOM: Διαχείριση Συστοιχιών Δίσκων . . . 532
40.1. Σύνοψη . . . 532
40.2. Εισαγωγή στο GEOM . . . 532
40.3. RAID0 - Striping . . . 532
40.4. RAID1 - Mirroring . . . 534
40.5. RAID3 - Striping σε Επίπεδο Byte με Αφοσιωμένο Parity . . . 538

40.6. Δικτυακές Συσκευές μέσω GEOM Gate . . . 540
40.7. Δημιουργώντας Ετικέτες (Labels) στις Συσκευές Δίσκων . . . 541
40.8. UFS Journaling Μέσω GEOM . . . 544
41. Υποστήριξη Συστημάτων Αρχείων . . . 547
41.1. Σύνοψη . . . 547
41.2. Το Σύστημα Αρχείων Z (ZFS) . . . 547
41.3. Συστήματα Αρχείων Linux® . . . 559
42. Εικονικοποίηση . . . 561
42.1. Σύνοψη . . . 561
42.2. Το FreeBSD ως φιλοξενούμενο λειτουργικό . . . 561
42.3. Το FreeBSD ως Ξενιστής (Host) . . . 593
43. Τοπικές Ρυθμίσεις - Χρήση και ρύθμιση I18N/L10N . . . 597
43.1. Σύνοψη . . . 597
43.2. Βασικές Γνώσεις . . . 597
43.3. Χρήση των Τοπικών Ρυθμίσεων . . . 598
43.4. Μεταγλώττιση Προγραμμάτων I18N . . . 605
43.5. Τοπικές Ρυθμίσεις για Συγκεκριμένες Γλώσσες . . . 605
44. Ενημέρωση και Αναβάθμιση του FreeBSD . . . 609
44.1. Σύνοψη . . . 609
44.2. Ενημερώνοντας το FreeBSD . . . 610
44.3. Portsnap: Ένα Εργαλείο Ενημέρωσης της Συλλογής των Ports . . . 618
44.4. Ενημερώνοντας την Τεκμηρίωση . . . 619
44.5. Παρακολούθηση Ενός Κλάδου Ανάπτυξης . . . 625
44.6. Συγχρονίζοντας τον Πηγαίο σας Κώδικα . . . 629
44.7. Μεταγλωττίζοντας το Βασικό Σύστημα ("world") . . . 630
44.8. Διαγραφή Παρωχημένων Αρχείων, Καταλόγων και Βιβλιοθηκών . . . 650
44.9. Διαδικασία για Πολλαπλά Μηχανήματα . . . 651
45. DTrace . . . 653
45.1. Σύνοψη . . . 653
45.2. Διαφορές στην Υλοποίηση . . . 653
45.3. Ενεργοποίηση της Υποστήριξης DTrace . . . 654
45.4. Χρησιμοποιώντας το DTrace . . . 655
45.5. Η Γλώσσα D . . . 658
IV: Serial Communications . . . 659
46. Σύνοψη . . . 660
47. Εισαγωγή . . . 661
47.1. Ορολογία . . . 661
47.2. Θύρες και Καλώδια . . . 661
47.3. Ρύθμιση του Πυρήνα . . . 664
47.4. Ειδικά Αρχεία Συσκευών . . . 665
47.5. Ρυθμίσεις Σειριακών Θυρών . . . 665

48. Τερματικά . . . 667
48.1. Χρήσεις και Είδη Τερματικών . . . 667
48.2. Ρύθμιση . . . 669
48.3. Αντιμετώπιση Προβλημάτων Σύνδεσης . . . 671
49. Υπηρεσία Εισόδου μέσω Επιλογικής Σύνδεσης (dial-in) . . . 673
49.1. Εξωτερικά και Εσωτερικά Modems . . . 673
49.2. Κυκλώματα Σειριακής Διασύνδεσης . . . 674
49.3. Γρήγορη Επισκόπηση . . . 674
49.4. Αρχεία Ρυθμίσεων . . . 675
49.5. Ρυθμίσεις Μνήμης . . . 679
49.6. Αντιμετώπιση Προβλημάτων . . . 680
50. Υπηρεσία Επιλογικής Σύνδεσης . . . 683
50.1. Το τύπου Hayes Modem μου δεν Υποστηρίζεται, Τι Μπορώ να Κάνω; . . . 683
50.2. Πως Υποτίθεται Ότι θα Στείλω Αυτές τις AT Εντολές; . . . 683
50.3. Το Σύμβολο @ της Ικανότητας pn Δεν Λειτουργεί! . . . 684
50.4. Πως Μπορώ να Καλέσω Ένα Τηλεφωνικό Αριθμό Από την Γραμμή Εντολών; . . . 684
50.5. Πρέπει να Πληκτρολογώ το Ρυθμό bps Κάθε Φορά που το Κάνω Αυτό; . . . 685
50.6. Έχω Πρόσβαση σε Ένα Αριθμό Υπολογιστών Μέσω Ενός Εξυπηρετητή Τερματικών . . . 685
50.7. Μπορεί η Tip να Δοκιμάσει Περισσότερες Από Μια Γραμμές για κάθε Σύνδεση; . . . 685
50.8. Γιατί Πρέπει να Πιέσω Ctrl + P Δύο Φορές για να Στείλω το Συνδυασμό Ctrl + P Μια Φορά; . . . 686
50.9. Ξαφνικά Ότι Γράφω Εμφανίζεται με Κεφαλαία Γράμματα!! . . . 686
50.10. Πως Μπορώ να Μεταφέρω Αρχεία με την tip; . . . 687
50.11. Πως Μπορώ να Εκτελέσω το zmodem με την tip; . . . 687
51. Ρύθμιση της Σειριακής Κονσόλας . . . 688
51.1. Εισαγωγή . . . 688
51.2. Ρύθμιση Σειριακής Κονσόλας (Σύντομη Έκδοση) . . . 688
51.3. Ρύθμιση Σειριακής Κονσόλας . . . 689
51.4. Περίληψη . . . 693
51.5. Συμβουλές για την Σειριακή Κονσόλα . . . 694
51.6. Αλλαγή Κονσόλας μέσω του Φορτωτή Εκκίνησης . . . 696
51.7. Πιθανές Παγίδες . . . 697
52. PPP . . . 698
52.1. Σύνοψη . . . 698
52.2. Χρησιμοποιώντας το PPP Χρήστη . . . 698
52.3. Χρησιμοποιώντας το PPP του Πυρήνα . . . 712
52.4. Αντιμετώπιση Προβλημάτων σε Συνδέσεις PPP . . . 721
52.5. Χρησιμοποιώντας PPP μέσω Ethernet (PPPoE) . . . 725
52.6. Χρησιμοποιώντας PPP μέσω ATM (PPPoA) . . . 727
52.7. Χρησιμοποιώντας το SLIP . . . 731
53. Ηλεκτρονικό Ταχυδρομείο . . . 741

53.1. Σύνοψη . . . 741
53.2. Χρησιμοποιώντας το Ηλεκτρονικό Ταχυδρομείο . . . 742
53.3. Ρύθμιση του sendmail . . . 744
53.4. Αλλάζοντας τον Αντιπρόσωπο Μεταφοράς Ταχυδρομείου (MTA) . . . 747
53.5. Αντιμετώπιση Προβλημάτων . . . 750
53.6. Προχωρημένα Θέματα . . . 753
53.7. SMTP με UUCP . . . 756
53.8. Ρύθμιση Εξυπηρετητή Μόνο για Αποστολή . . . 758
53.9. Χρησιμοποιώντας το Mail Μέσω Επιλογικής (Dialup) Σύνδεσης . . . 759
53.10. Πιστοποίηση Αυθεντικότητας στο SMTP . . . 760
53.11. Προγράμματα Ταχυδρομείου για τον Χρήστη . . . 762
53.12. Χρησιμοποιώντας το fetchmail . . . 771
53.13. Χρησιμοποιώντας το procmail . . . 772
54. Εξυπηρετητές Δικτύου . . . 774
54.1. Σύνοψη . . . 774
54.2. The inetd"Super-Server" . . . 774
54.3. Network File System (NFS) . . . 779
54.4. Network Information System (NIS/YP) . . . 785
54.5. Automatic Network Configuration (DHCP) . . . 802
54.6. Domain Name System (DNS) . . . 807
54.7. Ο εξυπηρετητής HTTP Apache . . . 817
54.8. Πρωτόκολο Μεταφοράς Αρχείων (FTP) . . . 822
54.9. File and Print Services for Microsoft® Windows® clients (Samba) . . . 823
54.10. Συγχρονισμός Ρολογιού Συστήματος με NTP . . . 826
55. Firewalls . . . 830
55.1. Σύνοψη . . . 830
55.2. Βασικές Έννοιες των Firewalls . . . 830
55.3. Προγράμματα Firewall . . . 831
55.4. Το Packet Filter (PF) και το ALTQ του OpenBSD . . . 831
55.5. Το IPFILTER (IPF) Firewall . . . 835
55.6. IPFW . . . 858
56. Προχωρημένα Θέματα Δικτύωσης . . . 880
56.1. Σύνοψη . . . 880
56.2. Gateways and Routes . . . 880
56.3. Wireless Networking . . . 887
56.4. Bluetooth . . . 902
56.5. Bridging . . . 912
56.6. Diskless Operation . . . 914
56.7. ISDN . . . 921
56.8. Network Address Translation . . . 925
56.9. Parallel Line IP (PLIP) . . . 929

56.10. IPv6 . . . 931
56.11. Asynchronous Transfer Mode (ATM) . . . 936
56.12. Common Access Redundancy Protocol (CARP) . . . 937
Appendix A: Που θα Βρείτε το FreeBSD . . . 940
57. Εκδόσεις σε CDROM και DVD . . . 941
57.1. Retail Εκδόσεις . . . 941
57.2. CD και DVD διανομές . . . 941
57.3. Διανομείς . . . 942
58. Εξυπηρετητές FTP . . . 944
59. Ανώνυμο CVS . . . 951
59.1. Εισαγωγή . . . 951
59.2. Χρησιμοποιώντας Ανώνυμο CVS . . . 951
59.3. Παραδείγματα . . . 952
59.4. Άλλες Πηγές Πληροφοριών . . . 953
60. Χρησιμοποιώντας το CTM . . . 954
60.1. Γιατί Πρέπει να Χρησιμοποιήσω το CTM; . . . 954
60.2. Τι Χρειάζομαι για να Χρησιμοποιήσω το CTM; . . . 954
60.3. Χρησιμοποιώντας το CTM για Πρώτη Φορά . . . 955
60.4. Χρησιμοποιώντας το CTM στην Καθημερινή σας Ζωή . . . 955
60.5. Κρατώντας τις Τοπικές σας Αλλαγές . . . 956
60.6. Άλλες Ενδιαφέρουσες Επιλογές του CTM . . . 956
60.7. Μελλοντικά Σχέδια για το CTM . . . 957
60.8. Διάφορα . . . 957
60.9. CTM Mirrors . . . 957
61. Χρησιμοποιώντας το CVSup . . . 959
61.1. Εισαγωγή . . . 959
61.2. Εγκατάσταση . . . 959
61.3. Ρύθμιση του CVSup . . . 960
61.4. Εκτελώντας το CVSup . . . 964
61.5. Συλλογές Αρχείων τουCVSup . . . 965
61.6. Για Περισσότερες Πληροφορίες . . . 972
61.7. Τοποθεσίες CVSup . . . 973
62. Ετικέτες (Tags) για το CVS . . . 974
62.1. Ετικέτες Κλάδων (Branch Tags) . . . 974
62.2. Ετικέτες Εκδόσεων (Release Tags) . . . 977
63. Τοποθεσίες AFS . . . 981
64. Τοποθεσίες rsync . . . 982
Appendix B: Βιβλιογραφία . . . 984
B.1. Βιβλία & Περιοδικά σχετικά με το FreeBSD . . . 984
B.2. Οδηγοί χρήστη . . . 985
B.3. Οδηγοί διαχειριστή . . . 985

B.4. Οδηγοί προγραμματιστών . . . 985
B.5. Το εσωτερικό του λειτουργικού συστήματος . . . 986
B.6. Αναφορές ασφαλείας . . . 986
B.7. Αναφορές υλικού . . . 987
B.8. Ιστορία του UNIX® . . . 987
B.9. Περιοδικά και εφημερίδες . . . 988
Appendix C: Πηγές Πληροφόρησης στο Διαδίκτυο . . . 989
C.1. Λίστες Ηλεκτρονικού Ταχυδρομείου . . . 989
C.2. Usenet Newsgroups . . . 1008
C.3. Διακομιστές Ιστοσελίδων . . . 1009
C.4. Διευθύνσεις Ηλεκτρονικού Ταχυδρομείου . . . 1012
Appendix D: Κλειδιά PGP . . . 1013
D.1. Officers . . . 1013

Πρόλογος

Σε Ποιους Απευθύνεται Αυτό το Βιβλίο

Το πρώτο τμήμα αυτού του βιβλίου, οδηγεί τον νέο χρήστη στη διαδικασία εγκατάστασης του FreeBSD και τον εισάγει ομαλά στη φιλοσοφία και τον σχεδιασμό του UNIX®. Αυτό το τμήμα δεν έχει ιδιαίτερες απαιτήσεις. Αρκεί μόνο η διάθεση για εξερεύνηση ενός νέου συστήματος και η δυνατότητα αφομοίωσης των γνώσεων για το FreeBSD καθώς αυτές εισάγονται σταδιακά.

Αφού διαβάσετε το πρώτο τμήμα, το δεύτερο, κατά πολύ μεγαλύτερο τμήμα, περιλαμβάνει μια εκτενή αναφορά σε διάφορα θέματα που ενδιαφέρουν τους διαχειριστές συστημάτων FreeBSD. Μερικά από αυτά τα κεφάλαια είναι ευκολότερο να τα κατανοήσετε αν έχετε ήδη μελετήσει συγκεκριμένα τμήματα του βιβλίου. Όπου χρειάζεται κάτι τέτοιο, θα αναφέρεται στη σύνοψη του κεφαλαίου που μόλις ξεκινήσατε να διαβάζετε.

Για περισσότερες πηγές πληροφοριών, δείτε το Βιβλιογραφία.

Αλλαγές από την Τρίτη Έκδοση

Η τρέχουσα έκδοση του Εγχειριδίου στο διαδίκτυο, είναι το αποτέλεσμα της προσπάθειας πολλών εκατοντάδων εθελοντών στο διάστημα των τελευταίων 10 χρόνων. Οι πιο σημαντικές αλλαγές σε σχέση με την τρίτη έντυπη έκδοση του Εγχειριδίου (2004) φαίνονται παρακάτω:

- Το DTrace είναι ένα νέο κεφάλαιο με πληροφορίες σχετικά με αυτό το πανίσχυρο εργαλείο ανάλυσης απόδοσης.
- Το Υποστήριξη Συστημάτων Αρχείων είναι ένα νέο κεφάλαιο με πληροφορίες για συστήματα αρχείων τα οποία υποστηρίζονται από το FreeBSD αλλά αναπτύσσονται από άλλες ομάδες, όπως το ZFS από την Sun™.
- Το Έλεγχος Συμβάντων Ασφαλείας είναι ένα νέο κεφάλαιο με πληροφορίες σχετικά με τις νέες δυνατότητες και την χρήση του auditing στο FreeBSD.
- Το Εικονικοποίηση είναι ένα νέο κεφάλαιο με πληροφορίες σχετικά με την εγκατάσταση του FreeBSD σε λογισμικό εκτέλεσης εικονικών (virtual) μηχανημάτων.
- Το Εγκατάσταση του FreeBSD 9.x και Μεταγενέστερων Εκδόσεων FreeBSD 9.*x* και Μεταγενέστερων Εκδόσεων, είναι ένα νέο κεφάλαιο σχετικά με την εγκατάσταση του FreeBSD με τη βοήθεια του νέου προγράμματος bsdinstall.

Αλλαγές από τη Δεύτερη Έκδοση (2004)

Η τρίτη έκδοση αυτού του βιβλίου ήταν το αποτέλεσμα της προσπάθειας περισσότερων από δύο χρόνων από τα μέλη της Ομάδας Τεκμηρίωσης του FreeBSD. Η έντυπη έκδοση είχε τόσο μεγάλο μέγεθος, που κρίθηκε αναγκαίο να τυπωθεί σε δύο χωριστούς τόμους. Παρακάτω φαίνονται οι σημαντικότερες αλλαγές σε αυτή τη νέα έκδοση:

- Το Ρύθμιση και Βελτιστοποίηση επεκτάθηκε με νέες πληροφορίες για τη διαχείριση ενέργειας και πόρων του συστήματος μέσω ACPI, με περισσότερες πληροφορίες για το σύστημα `cron` και με

περισσότερες επιλογές παραμετροποίησης του πυρήνα του FreeBSD.

- Το Ασφάλεια επεκτάθηκε με νέες πληροφορίες για Δίκτυα VPN, για λίστες ελέγχου πρόσβασης αρχείων (ACLs) και περισσότερες συμβουλές σχετικά με την ασφάλεια του FreeBSD.
- Το Υποχρεωτικός Έλεγχος Πρόσβασης είναι ένα νέο κεφάλαιο σε αυτή την έκδοση. Εξηγεί τι είναι ο μηχανισμός MAC και πώς μπορεί να χρησιμοποιηθεί για να ενισχυθεί η ασφάλεια ενός συστήματος FreeBSD.
- Το Αποθηκευτικά Μέσα επεκτάθηκε, με νέες πληροφορίες για συσκευές αποθήκευσης USB, στιγμιότυπα συστήματος αρχείων (snapshots), περιορισμούς στη χρήση των συστημάτων αρχείων (quotas), συστήματα αρχείων που βασίζονται σε υπάρχοντα αρχεία ή στο δίκτυο, καθώς και κρυπτογραφημένες κατατμήσεις δίσκων.
- Προστέθηκε μια ενότητα σχετικά με την αντιμετώπιση προβλημάτων στο PPP και SLIP.
- Το Ηλεκτρονικό Ταχυδρομείο επεκτάθηκε με νέες πληροφορίες για την χρήση εναλλακτικών MTA, πιστοποίηση ταυτότητας στο SMTP, το πρωτόκολλο UUCP, τα εργαλεία fetchmail και procmail και με άλλα θέματα για προχωρημένους.
- Το Εξυπηρετητές Δικτύου περιλαμβάνεται για πρώτη φορά σε αυτή την έκδοση. Αυτό το κεφάλαιο περιγράφει πως να εγκαταστήσετε τον Διακομιστή HTTP Apache, τον εξυπηρετητή ftpd του FreeBSD και τον διακομιστή Samba για επικοινωνία με πελάτες Microsoft® Windows®. Στο κεφάλαιο αυτό, έχουν μεταφερθεί κάποιες ενότητες από το Προχωρημένα Θέματα Δικτύωσης (Προχωρημένα Θέματα Δικτύωσης), προκειμένου να βελτιωθεί η παρουσίαση τους.
- Το Προχωρημένα Θέματα Δικτύωσης επεκτάθηκε με νέες πληροφορίες για τη χρήση συσκευών Bluetooth® στο FreeBSD, την εγκατάσταση ασύρματων δικτύων, και την Μέθοδο Δικτύωσης Ασύγχρονης Μεταφοράς (ATM).
- Προστέθηκε ένα Λεξιλόγιο, για να συγκεντρώσει όλους τους τεχνικούς όρους και τους διάφορους ορισμούς που περιέχονται σε ολόκληρο το βιβλίο.
- Έγιναν αισθητικές βελτιώσεις στους πίνακες και στα γραφήματα σε ολόκληρο το βιβλίο.

Αλλαγές από την Πρώτη Έκδοση (2001)

Η δεύτερη έκδοση ήταν το αποτέλεσμα τουλάχιστον δύο χρόνων εργασίας από τα μέλη της Ομάδας Τεκμηρίωσης του FreeBSD. Οι πιο σημαντικές αλλαγές σε αυτή την έκδοση ήταν οι παρακάτω:

- Προστέθηκε ένα ολοκληρωμένο Ευρετήριο.
- Όλα τα γραφήματα σε ASCII αντικαταστάθηκαν από γραφικά διαγράμματα.
- Προστέθηκε μια τυποποιημένη σύνοψη σε κάθε κεφάλαιο, η οποία περιέχει μια σύντομη ανακεφαλαίωση των πληροφοριών που περιέχει το κεφάλαιο και τι αναμένεται να γνωρίζει από πριν ο αναγνώστης.
- Το περιεχόμενο αναδιοργανώθηκε σε τρία λογικά μέρη: "Ξεκινώντας με το FreeBSD", "Διαχείριση Συστήματος" και "Παραρτήματα".
- Το Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων ξαναγράφτηκε από την αρχή με πολλές εικόνες, ώστε να διευκολύνει τους χρήστες να κατανοήσουν το κείμενο.
- Το Βασικές Έννοιες στο UNIX® επεκτάθηκε ώστε να συμπεριλαμβάνει πρόσθετες πληροφορίες για τις διεργασίες (processes), τους δαίμονες (daemons), και τα σήματα (signals).

- Το Εγκατάσταση Εφαρμογών: Πακέτα και Ports επεκτάθηκε ώστε να συμπεριλαμβάνει πρόσθετες πληροφορίες για την διαχείριση προμεταγλωττισμένων πακέτων (packages).
- Το Το Σύστημα X Window ξαναγράφτηκε από την αρχή με έμφαση στην χρήση μοντέρνων τεχνολογιών, όπως τα περιβάλλοντα εργασίας KDE και GNOME σε XFree86™ 4.X.
- Το Η Διαδικασία Εκκίνησης του FreeBSD επεκτάθηκε με περισσότερες πληροφορίες.
- Το Αποθηκευτικά Μέσα ξαναγράφτηκε με βάση τα παλαιότερα δύο κεφάλαια "Δίσκοι" και "Αντίγραφα Ασφαλείας". Πιστεύουμε ότι τα θέματα αυτά είναι πιο ευκολονόητα όταν παρουσιάζονται μαζί σαν ένα κεφάλαιο. Προστέθηκε επίσης μια ενότητα για RAID (υλοποίηση μέσω υλικού ή λογισμικού).
- Το Σειριακές Επικοινωνίες αναδιοργανώθηκε από την αρχή και ενημερώθηκε για τις εκδόσεις FreeBSD 4.X/5.X.
- Το PPP και SLIP ενημερώθηκε σε σημαντικό βαθμό.
- Πολλοί νέοι τομείς προστέθηκαν στο Προχωρημένα Θέματα Δικτύωσης.
- Το Ηλεκτρονικό Ταχυδρομείο επεκτάθηκε για να συμπεριλαμβάνει περισσότερες πληροφορίες για τις ρυθμίσεις του sendmail.
- Το Συμβατότητα με Εκτελέσιμα του Linux επεκτάθηκε για να συμπεριλαμβάνει πληροφορίες για την εγκατάσταση της βάσης δεδομένων Oracle® και του SAP® R/3®.
- Στην δεύτερη έκδοση καλύπτονται επίσης τα παρακάτω νέα θέματα:
  - Ρύθμιση και Βελτιστοποίηση.
  - Πολυμέσα.

Οργάνωση Αυτού του Βιβλίου

Αυτό το βιβλίο χωρίζεται σε πέντε διακριτά λογικά τμήματα. Το πρώτο τμήμα, *Ξεκινώντας με το FreeBSD*, περιγράφει την εγκατάσταση και την βασική χρήση του FreeBSD. Ο προτεινόμενος τρόπος ανάγνωσης αυτού του τμήματος είναι ένα-ένα κεφάλαιο, με τη σειρά, προσπερνώντας κεφάλαια με γνωστά θέματα. Το δεύτερο τμήμα, *Βασικές Εργασίες*, περιγράφει μερικά χαρακτηριστικά του FreeBSD τα οποία χρησιμοποιούνται συχνά. Μπορείτε να διαβάσετε τα κεφάλαια σε αυτό το τμήμα (καθώς και σε όλα τα τμήματα που ακολουθούν) με όποια σειρά θέλετε. Κάθε κεφάλαιο ξεκινά με μια σαφή και σύντομη σύνοψη, η οποία περιγράφει τα περιεχόμενα του κεφαλαίου καθώς και τι χρειάζεται να γνωρίζει ήδη ο αναγνώστης. Αυτό επιτρέπει στον περιστασιακό αναγνώστη να προσπερνά γρήγορα ενότητες, για να βρει κεφάλαια τα οποία τον ενδιαφέρουν περισσότερο. Το τρίτο τμήμα, *Διαχείριση Συστήματος*, περιέχει θέματα σχετικά με τη διαχείριση συστημάτων FreeBSD. Το τέταρτο τμήμα, *Δικτυακές Επικοινωνίες*, καλύπτει θέματα δικτύωσης και διακομιστών. Το πέμπτο τμήμα περιέχει παραρτήματα με διάφορες πληροφορίες.

Εισαγωγή

Παρουσιάζει το FreeBSD στο νέο χρήστη. Περιγράφει την ιστορία του FreeBSD Project, τους στόχους του και το μοντέλο ανάπτυξης του.

Εγκατάσταση του FreeBSD 9.x και Μεταγενέστερων Εκδόσεων

Οδηγεί τον χρήστη στην διαδικασία εγκατάστασης του FreeBSD 9.*x* και μεταγενέστερων εκδόσεων με τη χρήση του bsdinstall.

Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων

Οδηγεί τον χρήστη στην διαδικασία εγκατάστασης του FreeBSD 8.*x* και προγενέστερων εκδόσεων με τη χρήση του sysinstall. Συμπεριλαμβάνονται επίσης μερικά θέματα εγκατάστασης για προχωρημένους, όπως η εγκατάσταση μέσω σειριακής κονσόλας.

Βασικές Έννοιες στο UNIX®

Περιέχει τις βασικές εντολές και λειτουργίες του λειτουργικού συστήματος FreeBSD. Εάν είστε εξοικειωμένος με το Linux® ή με άλλο λειτουργικό τύπου UNIX® μπορείτε πιθανώς να προσπεράσετε αυτό το κεφάλαιο.

Εγκατάσταση Εφαρμογών: Πακέτα και Ports

Περιγράφει τον τρόπο εγκατάστασης λογισμικού τρίτων κατασκευαστών με την καινοτόμο "Συλλογή των Ports (Ports Collection)" του FreeBSD και με τα συνήθη προμεταγλωττισμένα πακέτα (packages).

Το Σύστημα X Window

Περιγράφει γενικά το σύστημα X Window και ειδικότερα το X11 του FreeBSD. Επίσης περιγράφει ολοκληρωμένα περιβάλλοντα εργασίας όπως το KDE και το GNOME.

Desktop Εφαρμογές

Αναφέρει και εξηγεί μερικές από τις πιο συνήθεις εφαρμογές για υπολογιστές γραφείου, όπως προγράμματα πλοήγησης ιστοσελίδων και εφαρμογές γραφείου και περιγράφει πως να τις εγκαταστήσετε στο FreeBSD.

Πολυμέσα

Υποδεικνύει πως να εγκαταστήσετε δυνατότητες αναπαραγωγής ήχου και βίντεο στο σύστημα σας. Επίσης περιλαμβάνει δειγματοληπτικά κάποιες εφαρμογές ήχου και βίντεο.

Ρυθμίζοντας τον Πυρήνα του FreeBSD

Εξηγεί τους λόγους για τους οποίους θα πρέπει να δημιουργήσετε ένα νέο πυρήνα. Παρέχει, επίσης, λεπτομερείς οδηγίες για την ρύθμιση, μεταγλώττιση και εγκατάσταση του νέου σας προσαρμοσμένου πυρήνα.

Εκτυπώσεις

Περιγράφει πως να διαχειρίζεστε εκτυπωτές στο FreeBSD. Συμπεριλαμβάνει πληροφορίες για σελίδες λογοτύπων, λογαριασμούς εκτυπωτών και αρχικές ρυθμίσεις.

Συμβατότητα με Εκτελέσιμα του Linux

Περιγράφει τις δυνατότητες συμβατότητας του FreeBSD με εφαρμογές Linux®. Επίσης παρέχει λεπτομερείς οδηγίες εγκατάστασης για πολλές γνωστές εφαρμογές του Linux® όπως Oracle®, και Mathematica®.

Ρύθμιση και Βελτιστοποίηση

Περιγράφει τις παραμέτρους που έχουν στη διάθεση τους οι διαχειριστές του συστήματος, ώστε να ρυθμίσουν ένα σύστημα FreeBSD για βέλτιστη απόδοση. Επίσης περιγράφει τα διάφορα αρχεία ρυθμίσεων που χρησιμοποιούνται στο FreeBSD και που να τα βρείτε.

Η Διαδικασία Εκκίνησης του FreeBSD

Περιγράφει την διαδικασία εκκίνησης του FreeBSD και εξηγεί πως μπορούμε να την ελέγχουμε με τη βοήθεια επιλογών και ρυθμίσεων.

Χρήστες και Βασική Διαχείριση Λογαριασμών

Περιγράφει την δημιουργία και την διαχείριση των λογαριασμών χρηστών. Επίσης περιγράφει τρόπους με τους οποίους μπορούν να τεθούν περιορισμοί στους χρήστες όσο αφορά τη χρήση πόρων του συστήματος, καθώς και άλλες λειτουργίες διαχείρισης λογαριασμών.

Ασφάλεια

Περιγράφει διάφορα διαθέσιμα εργαλεία που θα σας βοηθήσουν να κρατήσετε το FreeBSD σύστημα σας ασφαλές. Συμπεριλαμβάνονται οι υλοποιήσεις Kerberos, IPsec και OpenSSH.

Jails

Περιγράφει το πλαίσιο λειτουργιών των jails και τις βελτιώσεις που παρέχουν σε σχέση με την παραδοσιακή chroot υποστήριξη του FreeBSD.

Υποχρεωτικός Έλεγχος Πρόσβασης

Εξηγεί τι είναι ο Υποχρεωτικός Έλεγχος Πρόσβασης (MAC) και πως ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί για την ασφάλιση ενός FreeBSD συστήματος.

Έλεγχος Συμβάντων Ασφαλείας

Περιγράφει τι είναι ο Έλεγχος Συμβάντων, πως μπορεί να εγκατασταθεί, να ρυθμιστεί και πως μπορούν να διερευνώνται και να παρακολουθούνται τα ίχνη του ελέγχου (audit trails).

Αποθηκευτικά Μέσα

Περιγράφει πως να διαχειρίζεστε μέσα αποθήκευσης και συστήματα αρχείων με το FreeBSD. Συμπεριλαμβάνονται φυσικοί δίσκοι, συστοιχίες RAID, οπτικά και μαγνητικά μέσα, εικονικοί δίσκοι μνήμης και δικτυακά συστήματα αρχείων.

GEOM: Διαχείριση Συστοιχιών Δίσκων

Περιγράφει τι είναι το πλαίσιο λειτουργιών GEOM στο FreeBSD και πως να ρυθμίσετε διάφορα επίπεδα RAID που υποστηρίζονται στο FreeBSD.

Υποστήριξη Συστημάτων Αρχείων

Εξετάζει την υποστήριξη μη-εγγενών συστημάτων αρχείων στο FreeBSD, όπως το Z File System της Sun™.

Εικονικοποίηση

Περιγράφει τι προσφέρουν τα συστήματα εικονικοποίησης και πως μπορούν να χρησιμοποιηθούν με το FreeBSD.

Τοπικές Ρυθμίσεις - Χρήση και ρύθμιση I18N/L10N

Περιγράφει πως να χρησιμοποιήσετε το FreeBSD σε γλώσσες εκτός της Αγγλικής. Καλύπτει την δυνατότητα τοπικών ρυθμίσεων τόσο σε επίπεδο συστήματος, όσο και σε επίπεδο εφαρμογών.

Ενημέρωση και Αναβάθμιση του FreeBSD

Εξηγεί τις διαφορές μεταξύ των εκδόσεων FreeBSD-STABLE, FreeBSD-CURRENT και των

επίσημων (RELEASE) εκδόσεων του FreeBSD. Περιγράφει ποιοι χρήστες ωφελούνται όταν ακολουθούν ένα σύστημα ανάπτυξης καθώς και τα απαιτούμενα για αυτό το σκοπό βήματα. Καλύπτει τις μεθόδους που μπορούν να χρησιμοποιήσουν οι χρήστες για να ενημερώσουν το σύστημα τους με τις τελευταίες διορθώσεις ασφαλείας.

DTrace

Περιγράφει την ρύθμιση και χρήση του εργαλείου DTrace της Sun™ στο FreeBSD. Το δυναμικό tracing μπορεί να βοηθήσει στον εντοπισμό προβλημάτων απόδοσης, παρέχοντας ανάλυση του συστήματος σε πραγματικό χρόνο.

Σειριακές Επικοινωνίες

Εξηγεί πως να συνδέσετε τερματικά και μόντεμ στο FreeBSD σύστημα σας, για χρήση τόσο σε εισερχόμενες όσο και σε εξερχόμενες συνδέσεις.

PPP και SLIP

Περιγράφει πως να χρησιμοποιήσετε τις τεχνολογίες PPP, SLIP, ή PPP μέσω Ethernet για να συνδεθείτε σε απομακρυσμένα συστήματα με το FreeBSD.

Ηλεκτρονικό Ταχυδρομείο

Εξηγεί τα διαφορετικά στοιχεία ενός διακομιστή ηλεκτρονικής αλληλογραφίας και εμβαθύνει σε θέματα απλών ρυθμίσεων για το πλέον δημοφιλές λογισμικό διακομιστή ηλεκτρονικής αλληλογραφίας: το sendmail.

Εξυπηρετητές Δικτύου

Παρέχει λεπτομερείς οδηγίες και παραδείγματα αρχείων ρύθμισης για να ρυθμίσετε το FreeBSD να ενεργεί ως δικτυακός εξυπηρετητής αρχείων, εξυπηρετητής ονομάτων τομέα (DNS), εξυπηρετητής δικτυακών πληροφοριών (NIS), η εξυπηρετητής συγχρονισμού ώρας (NTP).

Firewalls

Εξηγεί την φιλοσοφία που κρύβεται πίσω από τα firewalls (τείχη προστασίας) που βασίζονται σε λογισμικό και παρέχει λεπτομερείς πληροφορίες για τις ρυθμίσεις των διαφόρων firewalls που διατίθενται για το FreeBSD.

Προχωρημένα Θέματα Δικτύωσης

Περιγράφει πολλά προχωρημένα θέματα δικτύωσης, συμπεριλαμβανομένου του διαμοιρασμού μιας σύνδεσης Internet με άλλους υπολογιστές στο τοπικό σας δίκτυο (LAN), θέματα δρομολόγησης για προχωρημένους, ασύρματη δικτύωση, Bluetooth®, ATM, IPv6 και πολλά ακόμη.

Που θα Βρείτε το FreeBSD

Περιέχει λίστα με διάφορες πηγές για να αποκτήσετε το FreeBSD σε CD-ROM ή DVD, όπως επίσης και διάφορες τοποθεσίες στο Internet από όπου μπορείτε να κατεβάσετε και να εγκαταστήσετε το FreeBSD.

Βιβλιογραφία

Αυτό το βιβλίο αγγίζει πολλά διαφορετικά θέματα που μπορεί να σας κεντρίσουν το ενδιαφέρον για μια πιο λεπτομερή εξερεύνηση. Η βιβλιογραφία ταξινομεί σε κατηγορίες πολλά εξαιρετικά βιβλία τα οποία αναφέρονται στο κείμενο.

Πηγές Πληροφόρησης στο Διαδίκτυο

Περιγράφει πολλά φόρουμ που διατίθενται στους χρήστες του FreeBSD, ώστε να θέτουν ερωτήματα και να συμμετέχουν σε τεχνικές συζητήσεις για το FreeBSD.

Κλειδιά PGP

Καταγράφει τα δακτυλικά αποτυπώματα των κλειδιών PGP αρκετών μελών της Ομάδας Ανάπτυξης του FreeBSD.

Συμβάσεις που χρησιμοποιούνται σε αυτό το βιβλίο

Σε ολόκληρο το βιβλίο, χρησιμοποιούνται κάποιες τυπογραφικές συμβάσεις ώστε η μορφοποίηση του να είναι συνεπής και να είναι πιο ευανάγνωστο:

Τυπογραφικές Συμβάσεις

Πλάγια γραφή

Η *πλάγια* γραμματοσειρά χρησιμοποιείται για ονόματα αρχείων, URLs, κείμενο με έμφαση και για χρήση πρωτοεμφανιζόμενων τεχνικών όρων.

`Γραφή σταθερού πλάτους`

Η `σταθερού πλάτους` γραμματοσειρά χρησιμοποιείται για μηνύματα λάθους, εντολές, μεταβλητές περιβάλλοντος, ονομασίες των ports, ονόματα κεντρικών υπολογιστών, ονόματα χρηστών, ονόματα ομάδων, ονόματα συσκευών, μεταβλητές και αποσπάσματα κώδικα.

Έντονη γραφή

Η έντονη γραμματοσειρά χρησιμοποιείται για εφαρμογές, εντολές και πλήκτρα.

Είσοδος Δεδομένων από το Χρήστη

Η πληκτρολόγηση σημειώνεται με **έντονη** γραφή ώστε να ξεχωρίζει από το υπόλοιπο κείμενο. Συνδυασμοί πλήκτρων που πρέπει να πιεσθούν ταυτόχρονα σημειώνονται με `+' μεταξύ των πλήκτρων, όπως:

`Ctrl` + `Alt` + `Del`

Το οποίο σημαίνει πως ο χρήστης θα πρέπει να πιέσει τα πλήκτρα `Ctrl`, `Alt` και το πλήκτρο `Del` ταυτόχρονα.

Σε περίπτωση που κάποια πλήκτρα πρέπει να πιεσθούν με συγκεκριμένη σειρά, θα εμφανίζονται χωρισμένα με κόμματα:

`Ctrl` + `X`, `Ctrl` + `S`

Το οποίο σημαίνει πως ο χρήστης αναμένεται να πιέσει τα πλήκτρα `Ctrl` και `X` ταυτόχρονα και έπειτα να πιέσει τα πλήκτρα `Ctrl` και `S` ταυτόχρονα.

Παραδείγματα

Τα παραδείγματα που ξεκινούν με C:\> υποδηλώνουν μια εντολή MS-DOS®. Αυτές οι εντολές μπορούν να εκτελούνται από το παράθυρο "Γραμμής Εντολών" σε σύγχρονο περιβάλλον Microsoft® Windows®, εκτός αν αναφέρεται κάτι διαφορετικό.

```
E:\> tools\fdimage floppies\kern.flp A:
```

Τα παραδείγματα που ξεκινούν με # υποδηλώνουν μια εντολή που θα πρέπει να εκτελεστεί από τον υπερχρήστη (superuser) ενός συστήματος FreeBSD. Μπορείτε να συνδεθείτε σαν χρήστης `root` για να πληκτρολογήσετε την εντολή, ή να συνδεθείτε σαν κανονικός χρήστης και να χρησιμοποιήσετε την εντολή su(1) ώστε να αποκτήσετε προνόμια υπερχρήστη.

```
# dd if=kern.flp of=/dev/fd0
```

Τα παραδείγματα που ξεκινούν με % υποδηλώνουν μια εντολή που πρέπει να εκτελεστεί από ένα κανονικό χρήστη. Χρησιμοποιείται η σύνταξη C-shell για να θέσουμε μεταβλητές περιβάλλοντος και άλλες εντολές κελύφους, εκτός αν αναφέρεται κάτι διαφορετικό.

```
% top
```

Ευχαριστίες

Το βιβλίο που κρατάτε, παρουσιάζει τις προσπάθειες πολλών εκατοντάδων ανθρώπων από όλο τον κόσμο. Είτε μας ενημέρωσαν για τυπογραφικά λάθη, είτε μας έστειλαν ολόκληρα κεφάλαια, η συμβολή όλων ήταν χρήσιμη.

Μερικές εταιρείες υποστήριξαν την ανάπτυξη αυτού του εγγράφου μισθώνοντας συντάκτες να εργάζονται σε πλήρη απασχόληση, πληρώνοντας για την έκδοση, κτλ. Ειδικότερα, η BSDi (η οποία αργότερα αποκτήθηκε από την Wind River Systems) μίσθωσε μέλη του FreeBSD Documentation Project να εργάζονται σε πλήρη απασχόληση για την βελτίωση του βιβλίου, οδηγώντας στην πρώτη έντυπη έκδοση στα αγγλικά τον Μάρτιο του 2000 (ISBN 1-57176-241-8). Η εταιρεία Wind River Systems μίσθωσε τότε μερικούς επιπρόσθετους συντάκτες ώστε να κάνει βελτιώσεις στην δομή της έντυπης έκδοσης και να προσθέσει κάποια νέα κεφάλαια. Η αποκορύφωση αυτής της εργασίας ήταν η παρουσίαση της δεύτερης έντυπης έκδοσης, τον Νοέμβριο του 2001 (ISBN 1-57176-303-1). 1-57176-303-1). Το 2003-2004, η FreeBSD Mall, Inc, μίσθωσε αρκετούς συνεργάτες να βελτιώσουν το Εγχειρίδιο Χρήσης προς ετοιμασία της τρίτης έντυπης έκδοσης.

params: path: "/books/handbook/parti/" :leveloffset: +1

Part I: Εισαγωγή

Chapter 1. Σύνοψη

Ευχαριστούμε για το ενδιαφέρον σας για το FreeBSD! Το ακόλουθο κεφάλαιο καλύπτει διάφορες πτυχές του FreeBSD Project, όπως την ιστορία του, τους στόχους του, το μοντέλο ανάπτυξης, κ.τ.λ.

Μετά την ανάγνωση αυτού του κεφαλαίου, θα γνωρίζετε:

- Πως σχετίζεται το FreeBSD με άλλα λειτουργικά συστήματα Η/Υ.
- Την ιστορία του FreeBSD Project.
- Τους στόχους του FreeBSD Project.
- Τις βασικές αρχές του open-source μοντέλου ανάπτυξης του FreeBSD.
- Και φυσικά: από που προέρχεται το όνομα "FreeBSD".

Chapter 2. Καλώς ήλθατε στο FreeBSD!

Το FreeBSD είναι ένα λειτουργικό σύστημα βασισμένο στο 4.4BSD-Lite, το οποίο μπορεί να χρησιμοποιηθεί σε Η/Υ Intel (x86 και Itanium®), AMD64 και Sun UltraSPARC®. Σε εξέλιξη βρίσκεται επίσης η διαδικασία μεταφοράς του FreeBSD σε άλλες αρχιτεκτονικές. Μπορείτε επίσης να διαβάσετε για την ιστορία του FreeBSD, ή για την πιο πρόσφατη επίσημη έκδοση του. Εάν ενδιαφέρεστε να συμβάλλετε με κάποιο τρόπο στο Project (κώδικα, hardware, χρηματοδότηση), διαβάστε το άρθρο Συνεισφέροντας στην Ανάπτυξη του FreeBSD.

2.1. Τι μπορεί να κάνει το FreeBSD;

Το FreeBSD έχει πολλά αξιόλογα χαρακτηριστικά. Μερικά από αυτά είναι:

- *Preemptive πολυεπεξεργασία* (preemptive multitasking) με δυναμικό έλεγχο προτεραιότητας για να εξασφαλιστεί ομαλός και δίκαιος διαμοιρασμός των πόρων του Η/Υ μεταξύ εφαρμογών και χρηστών, ακόμη και στις πιο αντίξοες συνθήκες και βαρύ φορτίο.
- *Πολυχρηστικές δυνατότητες* (multi-user facilities) οι οποίες επιτρέπουν σε πολλά άτομα ταυτόχρονα να χρησιμοποιήσουν ένα σύστημα FreeBSD για διαφορετικά πράγματα. Αυτό σημαίνει, για παράδειγμα, ότι τα περιφερειακά του συστήματος, όπως εκτυπωτές και οδηγοί ταινιών είναι σωστά μοιρασμένα μεταξύ όλων των χρηστών του συστήματος ή του δικτύου και πως μπορούν να τεθούν συγκεκριμένα όρια σε χρήστες ή ομάδες χρηστών, προστατεύοντας κρίσιμους πόρους του συστήματος από υπερβολική χρήση.
- Ισχυρές δυνατότητες *δικτύωσης TCP/IP* (TCP/IP networking) με υποστήριξη για βιομηχανικά πρότυπα όπως τα SCTP, DHCP, NFS, NIS, PPP, SLIP, IPsec και IPv6. Αυτό σημαίνει πως ένα μηχάνημα FreeBSD μπορεί να αλληλεπιδρά εύκολα με άλλα συστήματα και να εργάζεται σαν εταιρικός εξυπηρετητής, υποστηρίζοντας λειτουργίες ζωτικής σημασίας, όπως NFS (απομακρυσμένη πρόσβαση σε αρχεία) και υπηρεσίες ηλεκτρονικού ταχυδρομείου (e-mail), ή την παρουσία του οργανισμού σας στο διαδίκτυο μέσω των υπηρεσιών WWW, FTP, routing και firewall (ασφάλειας).
- Η *προστασία της μνήμης* (memory protection) εξασφαλίζει ότι οι διάφορες εφαρμογές (ή οι χρήστες) δεν αλληλεπιδρούν μεταξύ τους. Μια εφαρμογή που παρουσιάζει κάποιο πρόβλημα δε μπορεί να επηρεάσει άλλες με κανέναν τρόπο.
- Το βιομηχανικό πρότυπο *X Window System* (X11R6) προσφέρει γραφικό περιβάλλον εργασίας (GUI) σε οποιοδήποτε μηχάνημα και διατίθεται με τον πλήρη πηγαίο κώδικα.
- *Συμβατότητα εκτελέσιμων* με πολλά προγράμματα που έχουν μεταγλωττιστεί για Linux, SCO, SVR4, BSDI και NetBSD.
- Χιλιάδες *έτοιμες-προς-εκτέλεση* εφαρμογές είναι διαθέσιμες από την συλλογή *ports* και *packages* για το FreeBSD. Γιατί να ψάχνετε στο διαδίκτυο όταν μπορείτε να τα βρείτε όλα εδώ;
- Στο διαδίκτυο είναι επίσης διαθέσιμες χιλιάδες πρόσθετες και *εύκολες στην προσαρμογή* εφαρμογές. Το FreeBSD έχει συμβατότητα πηγαίου κώδικα με τα πιο δημοφιλή εμπορικά συστήματα UNIX®, επομένως οι περισσότερες εφαρμογές χρειάζονται λίγες έως καθόλου μετατροπές για να μεταγλωττιστούν (compile).
- Η κατά απαίτηση σελιδοποίηση *εικονικής μνήμης* και το "ολοκληρωμένο VM/buffer cache" παρέχουν υψηλή απόδοση σε εφαρμογές με αυξημένες ανάγκες σε μνήμη, ενώ διατηρούν την

ικανοποιητική απόκριση του συστήματος στους άλλους χρήστες.

- Υποστήριξη *SMP* για μηχανήματα με πολλαπλές CPU.
- Πλήρης σειρά εργαλείων ανάπτυξης για *C*, *C++*. Στη Συλλογή των Ports και των έτοιμων πακέτων, θα βρείτε πολλές ακόμα γλώσσες προγραμματισμού, κατάλληλες τόσο για έρευνα όσο και για ανάπτυξη λογισμικού.
- *Η διαθεσιμότητα του πηγαίου κώδικα* ολόκληρου του συστήματος σημαίνει ότι έχετε τον υψηλότερο βαθμό ελέγχου στο περιβάλλον σας. Γιατί να είστε κλειδωμένοι σε ένα κλειστό σύστημα και να είστε εξαρτημένοι από τον προμηθευτή σας, όταν μπορείτε να έχετε ένα πραγματικά ανοιχτό σύστημα;
- Εκτεταμένη *online τεκμηρίωση*.
- *Και πολλά άλλα!*

Το FreeBSD βασίζεται στην έκδοση 4.4BSD-Lite του Computer Systems Research Group (CSRG) του Πανεπιστημίου της Καλιφόρνιας στο Berkeley, και συνεχίζει την διακεκριμένη παράδοση του στην ανάπτυξη συστημάτων BSD. Επιπρόσθετα στο εξαίρετο έργο που παρείχε το CSRG, το FreeBSD Project ξόδεψε πολλές χιλιάδες ώρες στη βελτιστοποίηση του συστήματος για μέγιστες επιδόσεις και αξιοπιστία σε καθημερινές καταστάσεις πραγματικού φόρτου εργασίας. Το FreeBSD προσφέρει απόδοση και αξιοπιστία ισάξια με αντίστοιχων εμπορικών συστημάτων και τα συνδυάζει με τελευταίες τεχνολογιές και χαρακτηριστικά που δεν υπάρχουν πουθενά αλλού.

Οι εφαρμογές στις οποίες μπορεί να χρησιμοποιηθεί το FreeBSD, πραγματικά περιορίζονται μόνο από την φαντασία σας. Από ανάπτυξη λογισμικού μέχρι αυτοματισμούς εργοστασίων, από απογραφή ειδών μέχρι την διόρθωση του αζιμούθιου απομακρυσμένων δορυφορικών κεραιών, εάν μπορεί να γίνει με ένα εμπορικό προϊόν UNIX®, είναι παραπάνω από πιθανό ότι μπορεί να γίνει και με το FreeBSD! Το FreeBSD επίσης ωφελείται σημαντικά από κυριολεκτικά χιλιάδες εφαρμογές υψηλής ποιότητας που αναπτύσσονται από κέντρα ερευνών και πανεπιστήμια σε όλο τον κόσμο, και συχνά διατίθενται σε χαμηλό κόστος ή δωρεάν. Το πλήθος των εμπορικών εφαρμογών που διατίθενται για το FreeBSD, αυξάνεται επίσης καθημερινά.

Ο πηγαίος κώδικας του ίδιου του FreeBSD είναι πλήρως διαθέσιμος, και έτσι το σύστημα μπορεί να προσαρμοστεί σε αφάνταστα υψηλό επίπεδο για ειδικές εφαρμογές ή projects, και με τρόπους γενικά μη πραγματοποιήσιμους σε άλλα λειτουργικά εμπορικών προμηθευτών. Παρακάτω θα βρείτε μερικά μόνο παραδείγματα από εφαρμογές στις οποίες χρησιμοποιείται αυτή τη στιγμή το FreeBSD:

- *Υπηρεσίες Ίντερνετ:* Το ισχυρό σύστημα δικτύωσης TCP/IP του FreeBSD, το αναδεικνύει σε ιδανική πλατφόρμα για μια μεγάλη γκάμα υπηρεσιών Ίντερνετ όπως:
  - Εξυπηρετητές ιστοσελίδων World Wide Web (κοινούς ή με ασφαλή σύνδεση [SSL])
  - Δρομολόγηση πρωτοκόλλων IPv4 και IPv6
  - Firewalls και πύλες NAT ("IP masquerading")
  - Εξυπηρετητές FTP
  - Εξυπηρετητές ηλεκτρονικού ταχυδρομείου
  - Και άλλα...
- *Εκπαίδευση:* Είστε φοιτητής πληροφορικής ή κάποιου σχετικού τομέα; Δεν υπάρχει καλύτερος τρόπος να μάθετε για λειτουργικά συστήματα, αρχιτεκτονικές Η/Υ, και συστήματα δικτύων από

την πρακτική εμπειρία και την σε βάθος γνώση που μπορεί να σας παρέχει το FreeBSD. Το μεγάλο πλήθος των δωρεάν διαθέσιμων πακέτων εφαρμογών CAD, γραφικής σχεδίασης, και μαθηματικών, κάνουν το FreeBSD εξαιρετικά χρήσιμο σε όσους το κύριο ενδιαφέρον τους στους υπολογιστές είναι να *κάνουν τη δουλειά τους*!

- *Έρευνα:* Με διαθέσιμο τον πηγαίο κώδικα ολόκληρου του συστήματος, το FreeBSD είναι μία εξαίρετη πλατφόρμα για την έρευνα στα λειτουργικά συστήματα όπως επίσης για άλλους κλάδους της πληροφορικής. Η φύση της ελεύθερης διάθεσης του FreeBSD επιτρέπει επίσης σε απομακρυσμένες ομάδες να συνεργάζονται σε ιδέες ή να μοιράζονται την ανάπτυξη εφαρμογών, χωρίς να ανησυχούν για άδειες χρήσης και χωρίς να περιορίζεται η δυνατότητα τους για ελεύθερη συζήτηση οποιουδήποτε θέματος σε ανοιχτές ομάδες συζήτησης (forums).
- *Δικτύωση:* Χρειάζεστε ένα καινούργιο router (δρομολογητή); Ένα εξυπηρετητή DNS; Ένα firewall για να κρατάτε τον κόσμο έξω από το εσωτερικό σας δίκτυο; Το FreeBSD μπορεί εύκολα να μετατρέψει εκείνο το παλιό PC που κάθεται αχρησιμοποίητο στην γωνία, σε ένα προηγμένο δρομολογητή με εξεζητημένες δυνατότητες φιλτραρίσματος πακέτων.
- *Embedded:* Το FreeBSD αποτελεί μια εξαιρετική πλατφόρμα για τη δημιουργία embedded συστημάτων. Με υποστήριξη για τις πλατφόρμες ARM®, MIPS® και PowerPC® και σε συνδυασμό με αξιόπιστη δικτύωση, προηγμένα χαρακτηριστικά και την ελεύθερη άδεια BSD το FreeBSD είναι ένα εξαιρετικό σημείο εκκίνησης για embedded συστήματα router, firewall και άλλα.
- *Desktop:* Το FreeBSD είναι μια εξαίρετη επιλογή για ένα οικονομικό desktop. Το FreeBSD σας επιτρέπει να επιλέξετε ανάμεσα σε πολλά ανοικτού κώδικα περιβάλλοντα εργασίας τα οποία περιλαμβάνουν το GNOME και το KDE. Το FreeBSD μπορεί να ξεκινήσει ακόμα και "diskless" (χωρίς σκληρό δίσκο), κάνοντας έτσι τους προσωπικούς σταθμούς εργασίας ακόμη πιο φτηνούς και ευκολότερους στη διαχείριση.
- *Ανάπτυξη Λογισμικού:* Το βασικό σύστημα του FreeBSD διατίθεται ολοκληρωμένο, με πλήρη σειρά εργαλείων ανάπτυξης, που περιλαμβάνουν ένα πλήρη C/C++ compiler και debugger.

Το FreeBSD είναι διαθέσιμο για δωρεάν κατέβασμα ή μπορείτε να το προμηθευτείτε σε CD-ROM ή DVD. Δείτε το Που θα Βρείτε το FreeBSD για περισσότερες πληροφορίες για το πως να αποκτήσετε το FreeBSD.

2.2. Ποιος χρησιμοποιεί FreeBSD;

Τα προηγμένα χαρακτηριστικά, η αποδεδειγμένη ασφάλεια και ο τακτικός κύκλος νέων εκδόσεων του FreeBSD, σε συνδυασμό με την ελεύθερη άδεια χρήσης του, το κάνουν ιδανικό ως πλατφόρμα για τη δημιουργία πολλών εμπορικών και ανοιχτών συσκευών και προϊόντων. Κάποιες από τις μεγαλύτερες εταιρίες στο χώρο του IT χρησιμοποιούν το FreeBSD:

- Apache - Το Apache Software Foundation χρησιμοποιεί το FreeBSD στα περισσότερα δημόσια συστήματα του, που συμπεριλαμβάνουν ένα από τα μεγαλύτερα αποθετήρια SVN στον κόσμο με περισσότερα από 1.4 εκατομμύρια commits.
- Apple - Το OS X δανείζεται πολλά στοιχεία από το FreeBSD για το υποσύστημα δικτύωσης και τα εργαλεία χρήστη (userland). Το iOS περιέχει επίσης στοιχεία που προέρχονται από το FreeBSD.
- Cisco - Οι συσκευές ασφαλείας IronPort και anti-spam χρησιμοποιούν ένα τροποποιημένο πυρήνα του FreeBSD.

- Citrix - Η σειρά συσκευών ασφαλείας NetScaler παρέχει load balancing στα επίπεδα 4-7, caching περιεχομένου, firewall σε επίπεδο εφαρμογών, ασφαλές VPN και υπηρεσίες mobile cloud σε συνδυασμό με την ισχύ του τερματικού του FreeBSD.
- Dell KACE - Οι συσκευές διαχείρισης συστημάτων KACE χρησιμοποιούν FreeBSD λόγω της σταθερότητας και επεκτασιμότητας του καθώς και της κοινότητας που στηρίζει την συνεχή ανάπτυξη του.
- Experts Exchange - Όλοι οι δημόσιοι εξυπηρετητές ιστοσελίδων χρησιμοποιούν FreeBSD με εκτεταμένη χρήση jails για την απομόνωση των περιβάλλοντων ανάπτυξης και ελέγχου, χωρίς την πρόσθετη επιβάρυνση της εικονικοποίησης (virtualization).
- Isilon - Τα επαγγελματικά συστήματα αποθήκευσης της Isilon βασίζονται στο FreeBSD. Η εξαιρετικά ελεύθερη άδεια του FreeBSD επέτρεψε στην Isilon να ενσωματώσει το δικό της κώδικα (με τα δικά της πνευματικά δικαιώματα) στον πυρήνα και να επικεντρώσει την προσπάθεια της στη δημιουργία του προϊόντος της, αντί να ξαναγράψει ένα λειτουργικό σύστημα από την αρχή.
- iXsystems - Η σειρά συσκευών αποθήκευσης TrueNAS βασίζεται στο FreeBSD. Εκτός από τα εμπορικά της προϊόντα, η iXsystems κατευθύνει επίσης την ανάπτυξη των projects ανοικτού λογισμικού PC-BSD και FreeNAS.
- Juniper - Το λειτουργικό σύστημα JunOS το οποίο χρησιμοποιείται σε όλες τις συσκευές δικτύωσης της Juniper (που περιλαμβάνουν routers, switches και συσκευές ασφαλείας) βασίζεται στο FreeBSD. Η Juniper είναι μια εταιρία που επιδεικνύει τη συμβιωτική σχέση μεταξύ του Project και των εμπορικών προιόντων. Οι βελτιώσεις που παράγονται στη Juniper ενσωματώνονται στο FreeBSD μειώνοντας έτσι την πολυπλοκότητα της μελλοντικής ενσωμάτωσης νέων χαρακτηριστικών του FreeBSD πίσω στο JunOS.
- McAfee - Το SecurOS, που αποτελεί τη βάση των προϊόντων firewall της εταιρίας και περιλαμβάνει το Sidewinder, βασίζεται στο FreeBSD.
- NetApp - Οι συσκευές αποθήκευσης Data ONTAP GX βασίζονται στο FreeBSD. Επιπρόσθετα, η NetApp έχει συνεισφέρει αρκετά νέα χαρακτηριστικά, συμπεριλαμβανομένου του bhyve, του νέου hypervisor ύπο άδεια BSD.
- Netflix - Η συσκευή OpenConnect που χρησιμοποιεί η Netflix για το streaming ταινιών στους πελάτες της, βασίζεται στο FreeBSD. Η Netflix έχει εκτεταμένη συνεισφορά στον κώδικα και εργάζεται ώστε να μην υπάρχουν διαφορές μεταξύ του κώδικα της και του FreeBSD. Οι συσκευές Netflix OpenConnect είναι υπεύθυνες για περισσότερο από το 32% της συνολικής κίνησης Internet στη Βόρειο Αμερική.
- Sandvine - Η Sandvine χρησιμοποιεί το FreeBSD ως βάση για την υψηλής απόδοσης δικτυακή πλατφόρμα επεξεργασίας που χρησιμοποιεί στα προϊόντα της.
- Sony - Η κονσόλα παιχνιδιών PlayStation 4 χρησιμοποιεί μια τροποποιημένη έκδοση του FreeBSD.
- Sophos - Η συσκευή Sophos Email Appliance χρησιμοποιεί μια ενισχυμένης ασφάλειας έκδοση του FreeBSD και σαρώνει τα εισερχόμενα email για spam και ιούς καθώς και τα εξερχόμενα για ανεπιθύμητα προγράμματα (malware) και πιθανή απώλεια ευαίσθητων δεδομένων.
- Spectra Logic - Η σειρά αποθηκευτικών μέσων nTier χρησιμοποιεί FreeBSD και OpenZFS.
- The Weather Channel - Η συσκευή IntelliStar που εγκαθίσταται στους παρόχους καλωδιακής τηλεόρασης και παρέχει δελτία καιρού στους συνδρομητές, χρησιμοποιεί FreeBSD.

- Verisign - Η Verisign είναι υπεύθυνη για τη λειτουργία των τομέων .com και .net και των αντίστοιχων εξυπηρετητών DNS. Χρησιμοποιεί διάφορα δικτυακά λειτουργικά συστήματα, συμπεριλαμβανομένου του FreeBSD, για να εξασφαλίσει ότι δεν μπορεί να υπάρξει κάποιο κοινό σημείο αποτυχίας στην δικτυακή υποδομή της.
- Voxer - Η Voxer χρησιμοποιεί το FreeBSD με ZFS στην πλατφόρμα μηνυμάτων που εχει αναπτύξει για κινητά τηλέφωνα. Η Voxer αρχικά χρησιμοποιούσε ένα σύστημα που προέρχονταν από το Solaris, αλλά το άλλαξε σε FreeBSD λόγω της εξαιρετικής του τεκμηρίωσης, της μεγαλύτερης και πιο ενεργής κοινότητας και του φιλικότερου περιβάλλοντος ανάπτυξης. Εκτός από τα ιδιαίτερα κρίσιμα χαρακτηριστικά - όπως το ZFS και το DTrace - το FreeBSD επίσης διαθέτει και υποστήριξη TRIM για το ZFS.
- WhatsApp - Όταν η WhatsApp χρειάστηκε μια πλατφόρμα ικανή να αντιμετωπίσει περισσότερες από 1 εκατομμύριο ταυτόχρονες συνδέσεις TCP ανά εξυπηρετητή, επέλεξαν το FreeBSD. Έπειτα πέτυχαν περισσότερες από 2.5 εκατομμύρια συνδέσεις ανά εξυπηρετητή.
- Wheel Systems - Η συσκευή ασφαλείας FUDO επιτρέπει στις επιχειρήσεις να ελέγχουν, να κατευθύνουν και να καταγράφουν διαχειριστές και εργαζομένους άλλων εταιριών που εργάζονται στα συστήματα τους. Βασίζεται στα καλύτερα χαρακτηριστικά ασφαλείας του FreeBSD που περιλαμβάνουν τεχνολογίες όπως ZFS, GELI, Capsicum, HAST και auditdstd.

Το FreeBSD έχει επίσης βοηθήσει στη δημιουργία και άλλων σχετιζόμενων έργων ανοικτού λογισμικού:

- BSD Router - Ένας εναλλακτικός router για μεγάλες επιχειρήσεις που χρησιμοποιεί FreeBSD και είναι σχεδιασμένος να λειτουργεί σε απλά PC της αγοράς.
- FreeNAS - Μια τροποποιημένη έκδοση του FreeBSD σχεδιασμένη για χρήση ως συσκευή δικτυακής αποθήκευσης. Παρέχει γραφική διεπαφή γραμμένη σε Python η οποία απλουστεύει τη διαχείριση των συστημάτων αρχείων UFS και ZFS. Περιλαμβάνει υποστήριξη για NFS, SMB/CIFS, AFP, FTP και iSCSI. Έχει δυνατότητα επέκτασης μέσω πρόσθετων (plugins) τα οποία βασίζονται σε FreeBSD jails.
- GhostBSD - Μια διανομή του FreeBSD για χρήση desktop. Παρέχεται με το περιβάλλον εργασίας Gnome.
- mfsBSD - Ένα σύνολο εργαλείων για τη δημιουργία ενός συστήματος FreeBSD το οποίο εκτελείται αποκλειστικά από τη μνήμη.
- NAS4Free - Μια διανομή για εξυπηρετητές αρχείων που βασίζεται στο FreeBSD και παρέχεται με μια web διεπαφή ρυθμίσεων γραμμένη σε PHP.
- PC-BSD - Μια τροποποιημένη διανομή του FreeBSD που προσανατολίζεται σε χρήση desktop και παρέχει γραφικά εργαλεία για να αναδείξει τη δύναμη του FreeBSD σε όλους τους χρήστες. Είναι σχεδιασμένη ώστε να διευκολύνει τη μετάβαση των χρηστών Windows και OS X στο FreeBSD.
- pfSense - Μια διανομή για firewall που βασίζεται στο FreeBSD και περιέχει τεράστια συλλογή χαρακτηριστικών και εκτεταμένη υποστήριξη για IPv6.
- m0n0wall - Μια λιτή έκδοση του FreeBSD με ένα εξυπηρετητή ιστοσελίδων και διεπαφή σε PHP. Έχει σχεδιαστεί ως συσκευή firewall και καταλαμβάνει χώρο μικρότερο από 12 MB.
- ZRouter - Ένα εναλλακτικό firmware ανοικτού λογισμικού για δικτυακές συσκευές, βασισμένο στο FreeBSD. Έχει σχεδιαστεί ώστε να αντικαθιστά το ιδιοταγές firmware εμπορικών routers.

Το FreeBSD χρησιμοποιείται για να υποστηρίζει μερικές από τις μεγαλύτερες τοποθεσίες στο Ίντερνετ, περιλαμβανομένων των:

- Yahoo!
- Yandex
- Rambler
- Sina
- Pair Networks
- Sony Japan
- Netcraft
- Netflix
- NetEase
- Weathernews
- TELEHOUSE America

και πολλών ακόμη. Στη Wikipedia θα βρείτε μια λίστα προϊόντων που βασίζονται στο FreeBSD.

Chapter 3. Πληροφορίες για το FreeBSD Project

Το ακόλουθο τμήμα παρέχει μερικές πληροφορίες σχετικές με το project, και περιλαμβάνει μια σύντομη ιστορία του FreeBSD, τους στόχους, και το μοντέλο ανάπτυξης του.

3.1. Μια σύντομη ιστορία του FreeBSD

Το FreeBSD Project γεννήθηκε στις αρχές του 1993, μερικώς σαν εξέλιξη του "Unofficial 386BSD Patchkit" από τους 3 τελευταίους συντονιστές του patchkit: τον Nate Williams, τον Rod Grimes και τον Jordan Hubbard.

Ο πρωταρχικός στόχος ήταν να παραχθεί ένα ενδιάμεσο στιγμιότυπο (snapshot) του 386BSD ώστε να διορθωθούν μερικά προβλήματα που ο μηχανισμός του patchkit δεν ήταν ικανός να λύσει. Ο αρχικός τίτλος εργασίας για το project ήταν "386BSD 0.5" ή "386BSD Interim" και αναφέρονταν σε αυτό ακριβώς το γεγονός.

Το 386BSD ήταν το λειτουργικό σύστημα του Bill Jolitz, το οποίο μέχρι εκείνο το σημείο, υπέφερε βαριά έχοντας αμεληθεί για σχεδόν ένα έτος. Καθώς το patchkit φούσκωνε ολοένα και περισσότερο με το πέρασμα των ημερών, το ενδιάμεσο "cleanup" snapshot αποτέλεσε μια συμπαράσταση για τον Bill. Τα σχέδια αυτά διακόπηκαν απότομα, όταν ξαφνικά ο Bill Jolitz αποφάσισε να αποσύρει την έγκριση του στο project δίχως μια ξεκάθαρη ένδειξη του τι θα έπρεπε να γίνει.

Οι τρεις συντονιστές γρήγορα αποφάσισαν πως ο στόχος παρέμενε αξιόλογος, ακόμη και χωρίς την βοήθεια του Bill, και έτσι υιοθέτησαν το όνομα "FreeBSD", που επινόησε ο David Greenman. Οι αρχικοί στόχοι τέθηκαν κατόπιν συμβουλών από τους τότε χρήστες του συστήματος, και όταν έγινε πλέον ξεκάθαρο πως το project είχε πάρει σωστή πορεία και ίσως έτεινε να γίνει πραγματικότητα, ο Jordan ήρθε σε επαφή με την Walnut Creek CDROM προσβλέποντας στην βελτίωση των καναλιών διανομής του FreeBSD για όλους αυτούς τους άτυχους που δεν είχαν εύκολη πρόσβαση στο Ίντερνετ. Η Walnut Creek CDROM, όχι μόνο υποστήριξε την ιδέα διανομής του FreeBSD σε CD, αλλά προχώρησε αρκετά περισσότερο, παρέχοντας στο project ένα μηχάνημα εργασίας και μια γρήγορη σύνδεση στο Ίντερνετ. Δίχως τον βαθμό πίστης της Walnut Creek CDROM σε αυτό που εκείνο τον καιρό ήταν ένα εντελώς άγνωστο project, είναι πολύ απίθανο το FreeBSD να είχε φτάσει τόσο μακριά, και τόσο γρήγορα, όπως σήμερα.

Η πρώτη διανομή CD-ROM (και με γενικά ευρεία διάδοση στο δίκτυο) ήταν η FreeBSD 1.0, που κυκλοφόρησε τον Δεκέμβρη του 1993. Βασίζονταν σε μια ταινία του 4.3BSD-Lite ("Net/2") του U.C. Berkeley, έχοντας πάρει και πολλά στοιχεία από το 386BSD και το Free Software Foundation. Ήταν αρκετά επιτυχημένη για πρώτη προσπάθεια, και την συνεχίσαμε με την αρκετά επιτυχημένη έκδοση FreeBSD 1.1 που κυκλοφόρησε τον Μάϊο του 1994.

Περίπου εκείνη την περίοδο, σχηματίστηκαν απρόσμενα στον ορίζοντα σύννεφα καταιγίδας, καθώς η Novell και το U.C. Berkeley τακτοποίησαν την μακράς διαρκείας δικαστική διαμάχη σχετικά με τα δικαιώματα της ταινίας Net/2. Μία συνθήκη αυτής της συμφωνίας ήταν η παραδοχή από την μεριά του U.C. Berkeley ότι μεγάλο μέρος του Net/2 ήταν "επιβαρυμένος" κώδικας και ιδιοκτησία της Novell, η οποία με την σειρά της το είχε αποκτήσει από την AT&T λίγο καιρό πριν. Αυτό που πήρε ως αντάλλαγμα το Berkeley ήταν οι "ευλογίες" της Novell ότι η έκδοση 4.4BSD-Lite, όταν τελικά

ολοκληρωνόταν, θα δηλωνόταν ως μη-επιβαρυμένη, και όλοι οι μέχρι τότε χρήστες του Net/2 θα ενθαρρύνονταν ένθερμα να μεταβούν σε αυτή. Αυτό συμπεριλάμβανε και το FreeBSD, και στο project δόθηκε χρόνος μέχρι τον Ιούλιο του 1994 να σταματήσει τις παραδόσεις των προϊόντων που βασίζονταν στο Net/2. Υπό τους όρους αυτής της συμφωνίας, επιτράπηκε στο project μια τελευταία έκδοση πριν την λήξη της προθεσμίας, και αυτή ήταν η έκδοση FreeBSD 1.1.5.1.

Το FreeBSD βρέθηκε τότε στη δυσχερή θέση κυριολεκτικά να ξανα-ανακαλύψει τον εαυτό του από ένα σύνολο από bit του 4.4BSD-Lite, εντελώς καινούργιο, και κυρίως ατελές. Οι εκδόσεις "Lite" ήταν light (ελαφριές) εν' μέρει επειδή το CSRG του Berkeley είχε αφαιρέσει μεγάλο όγκο κώδικα ο οποίος ήταν απαραίτητος για να κατασκευαστεί ένα πραγματικά εκκινήσιμο λειτουργικό σύστημα (λόγω διαφόρων νομικών ζητημάτων), και εν' μέρει επειδή το port για Intel του 4.4 ήταν σε υψηλό βαθμό ατελές. Η μετάβαση ολοκληρώθηκε τον Νοέμβριο του 1994, και σε αυτό το σημείο κυκλοφόρησε η FreeBSD 2.0. Παρά το γεγονός ότι ήταν ακόμη αρκετά πρόχειρη μέσες-άκρες, η έκδοση ήταν μια σημαντική επιτυχία και την ακολούθησε η πιο αξιόπιστη και ευκολότερη ως προς την εγκατάσταση έκδοση FreeBSD 2.0.5 τον Ιούνιο του 1995.

Από την εποχή εκείνη, το FreeBSD έχει δημιουργήσει σειρά νέων εκδόσεων οι οποίες βελτιώνουν την ταχύτητα, σταθερότητα και τα χαρακτηριστικά των προηγούμενων.

Για την ώρα, η μακρόχρονη ανάπτυξη συνεχίζεται στον κλάδο 10.X-CURRENT (trunk) και τα στιγμιότυπα (snapshots) του 10.X είναι πάντοτε διαθέσιμα μέσω του εξυπηρετητή snapshot.

3.2. Στόχοι του FreeBSD Project

Οι στόχοι του FreeBSD Project είναι να παρέχει λογισμικό που θα μπορεί να χρησιμοποιηθεί για οποιαδήποτε περίσταση και δίχως δεσμεύσεις. Πολλοί από μας έχουν κάνει σημαντική επένδυση στον κώδικα (και το project) και σίγουρα δε θα μας πείραζε πότε-πότε μια μικρή οικονομική συνεισφορά, αλλά σίγουρα δεν είμαστε έτοιμοι να επιμείνουμε σε αυτό. Πιστεύουμε ότι η πρωταρχική και σπουδαιότερη "αποστολή" μας είναι να παρέχουμε κώδικα σε υπάρχοντες και μελλοντικούς χρήστες, και για οποιοδήποτε σκοπό, ώστε ο κώδικας μας να έχει την ευρύτερη πιθανή χρήση και να αποφέρει το μεγαλύτερο δυνατό όφελος. Αυτό είναι, πιστεύω, ένας από τους σημαντικότερους στόχους του Ελεύθερου Λογισμικού και ένας από τους οποίους υποστηρίζουμε με ενθουσιασμό.

Το τμήμα του πηγαίου μας κώδικα που βρίσκεται υπό την GNU General Public License (GPL) ή την Library General Public License (LGPL) έχει κάπως περισσότερες δεσμεύσεις, αν και σκοπός τους είναι μάλλον να διασφαλίσουν την ελεύθερη διάθεση του κώδικα, παρά το αντίθετο. Λόγω των επιπρόσθετων επιπλοκών που θέτει η άδεια χρήσης GPL στην εμπορική χρήση του λογισμικού, προτιμούμε, όσο είναι εφικτό, να παρέχουμε το λογισμικό μας υπό το χαλαρότερο BSD copyright.

3.3. Το Μοντέλο Ανάπτυξης του FreeBSD

Η ανάπτυξη του FreeBSD είναι μία πολύ ανοικτή και ευέλικτη διαδικασία, αφού κυριολεκτικά βασίζεται στην συνεισφορά χιλιάδων ανθρώπων από όλο τον κόσμο, όπως μπορείτε να δείτε από την λίστα των συνεργατών μας. Η υποδομή ανάπτυξης του FreeBSD επιτρέπει στα χιλιάδες μέλη των συνεργατών μας να συνεργάζονται μέσω του Ίντερνετ. Είμαστε σταθερά σε αναζήτηση για νέα μέλη στην ομάδα ανάπτυξης και για ιδέες, και όσοι ενδιαφέρονται να ασχοληθούν ακόμη περισσότερο με το project χρειάζεται απλά να επικοινωνήσουν μαζί μας στην ηλεκτρονική λίστα τεχνικών

συζητήσεων του FreeBSD. Επίσης η ηλεκτρονική λίστα ανακοινώσεων του FreeBSD είναι διαθέσιμη σε όσους επιθυμούν να ενημερώσουν άλλους χρήστες του FreeBSD για βασικούς τομείς εργασίας πάνω στο Project.

Χρήσιμα πράγματα που πρέπει να γνωρίζετε για το FreeBSD Project και την διαδικασία ανάπτυξης του, είτε δουλεύετε ανεξάρτητα είτε ως στενοί συνεργάτες:

Τα SVN repositories

Για πολλά χρόνια, ο κεντρικός κορμός κώδικα του FreeBSD συντηρούνταν μέσω του CVS (Concurrent Versions System), ενός ελεύθερα διαθέσιμου εργαλείου ελέγχου πηγαίου κώδικα. Τον Ιούνιο του 2008, το Project αποφάσισε τη μετάβαση στο SVN (Subversion). Η αλλαγή κρίθηκε αναγκαία, καθώς οι τεχνικοί περιορισμοί του CVS ήταν πλέον εμφανείς, εξαιτίας του μεγέθους του αποθηκευμένου κώδικα και του ιστορικού που τον συνοδεύει. Η Τεκμηρίωση και η Συλλογή των Ports μεταφέρθηκαν επίσης από το CVS στο SVN το Μάιο και Ιούλιο του 2012 αντίστοιχα. Ακολουθήστε το σύνδεσμο Συγχρονίζοντας τον Πηγαίο σας Κώδικα για περισσότερες πληροφορίες σχετικά με την ανάκτηση του FreeBSD `src/` repository και τον σύνδεσμο Χρησιμοποιώντας τη Συλλογή των Ports για λεπτομέρειες σχετικές με την ανάκτηση της Συλλογής των Ports.

Η λίστα των committers

Οι *committers* είναι άτομα που έχουν άδεια *εγγραφής (write)* στο δέντρο Subversion και είναι εξουσιοδοτημένοι να κάνουν μετατροπές στον κώδικα του FreeBSD (ο όρος "committer" προέρχεται από την εντολή `commit`, η οποία χρησιμοποιείται για να γίνουν νέες αλλαγές στο repository). Οποιοσδήποτε μπορεί να υποβάλλει ένα σφάλμα (bug) στη Βάση Δεδομένων Προβλημάτων. Πριν την υποβολή, καλό είναι να γίνει σχετική αναζήτηση στις λίστες ταχυδρομείου, τα φορουμς και τα κανάλια IRC του FreeBSD για να επιβεβαιωθεί ότι όντως πρόκειται για πρόβλημα του λειτουργικού.

The FreeBSD core team

Η *FreeBSD core team* θα ήταν ισοδύναμη με το διοικητικό συμβούλιο αν το FreeBSD Project ήταν μια ανώνυμη εταιρεία. Ο πρωταρχικός στόχος της core team είναι να εξασφαλίσει ότι το project, στο σύνολο του, είναι σε καλή κατάσταση και να το οδηγεί προς την σωστή κατεύθυνση. Μια από τις λειτουργίες της core team είναι να προσκαλεί αφοσιωμένους και υπεύθυνους developers να συμμετέχουν στην ομάδα ανάπτυξης (τους committers) καθώς και να βρίσκει νέα μέλη για την ίδια την core team καθώς κάποιοι αποχωρούν. Η παρούσα core team εκλέχτηκε από ένα σύνολο υποψηφίων committers τον Ιούλιο του 2014. Εκλογές διεξάγονται κάθε 2 χρόνια.

Όπως και τα περισσότερη μέλη της ομάδας ανάπτυξης, τα περισσότερα μέλη του core team είναι εθελοντές όσον αφορά την ανάπτυξη του FreeBSD και δεν έχουν οικονομικής φύσεως οφέλη από το project, επομένως η "δέσμευση" δεν θα πρέπει να παρερμηνεύεται ως "εγγυημένη υποστήριξη". Η παραπάνω παρομοίωση με το "διοικητικό συμβούλιο" δεν είναι πολύ ακριβής, ίσως είναι καταλληλότερο να πούμε ότι πρόκειται για ανθρώπους που θυσίασαν τις ζωές τους για χάρη του FreeBSD ενάντια στην καλύτερη τους κρίση!

Εξωτερικοί συνεργάτες

Τέλος, αλλά οπωσδήποτε όχι μικρότερης σημασίας, η μεγαλύτερη ομάδα ανάπτυξης είναι οι ίδιοι οι χρήστες που μας παρέχουν σχόλια και διορθώσεις των bug σε σχεδόν σταθερή βάση. Ο κύριος

τρόπος για να κρατάτε επαφή με την μη-συγκεντρωτική ομάδα ανάπτυξης του FreeBSD είναι να γίνετε συνδρομητές στην ηλεκτρονική λίστα τεχνικών συζητήσεων του FreeBSD όπου γίνονται οι ανάλογες συζητήσεις. Δείτε το Πηγές Πληροφόρησης στο Διαδίκτυο για περισσότερες πληροφορίες σχετικά με τις διάφορες λίστες ηλεκτρονικού ταχυδρομείου του FreeBSD.

Η Λίστα Συνεργατών του FreeBSD είναι μεγάλη και συνεχώς αυξανόμενη, επομένως γιατί να μην γίνετε και εσείς μέλος της και να συμβάλλετε σήμερα σε κάτι στο FreeBSD;

Η παροχή κώδικα δεν είναι ο μόνος τρόπος για να συνεισφέρετε στο project. Για μια ολοκληρωμένη λίστα των πραγμάτων στα οποία χρειαζόμαστε βοήθεια, παρακαλούμε επισκεφθείτε την Δικτυακή τοποθεσία του FreeBSD Project.

Συνοψίζοντας, το μοντέλο ανάπτυξης μας είναι οργανωμένο σαν ένα χαλαρό σύνολο ομόκεντρων κύκλων. Το συγκεντρωτικό μοντέλο είναι σχεδιασμένο για να διευκολύνει τους *χρήστες* του FreeBSD, στους οποίους παρέχεται έτσι ένας εύκολος τρόπος παρακολούθησης του βασικού κώδικα, και όχι για να αποκλείουμε πιθανούς συνεργάτες! Επιθυμία μας είναι να παρουσιάσουμε ένα σταθερό λειτουργικό σύστημα σε συνάρτηση με μια μεγάλη γκάμα από προγράμματα εφαρμογών που οι χρήστες να μπορούν εύκολα να εγκαθιστούν και να χρησιμοποιούν - για την εκπλήρωση αυτών των στόχων, το μοντέλο αυτό δουλεύει πολύ καλά.

Το μόνο που ζητάμε από όσους ενδιαφέρονται να ενωθούν μαζί μας στην ομάδα ανάπτυξης του FreeBSD, είναι λίγη από την ίδια αφοσίωση της τωρινής ομάδας, για μια συνεχή πορεία στην επιτυχία του!

3.4. Προγράμματα Τρίτων Κατασκευαστών

Εκτός από τη βασική του διανομή, το FreeBSD προσφέρει μια συλλογή λογισμικού με χιλιάδες προγράμματα για καθημερινή χρήση. Την στιγμή που γράφονται αυτές οι γραμμές, υπάρχουν πάνω από 36000 ports! Η λίστα των ports ξεκινάει από εξυπηρετητές http (WWW), μέχρι παιχνίδια, γλώσσες προγραμματισμού, κειμενογράφους, και οτιδήποτε άλλο ενδιάμεσα. Η συνολική Συλλογή των Ports απαιτεί προσεγγιστικά 3 GB. Για να μεταγλωττιστεί (compile) ένα port, χρειάζεται απλώς να μεταβείτε στον κατάλογο του προγράμματος που επιθυμείτε να εγκαταστήσετε, να πληκτρολογήσετε `make install`, και να αφήσετε το σύστημα σας να κάνει τα υπόλοιπα. Ολόκληρη η αυθεντική διανομή για κάθε port που κάνετε build παρέχεται δυναμικά έτσι τα ports που δεν χρειάζεστε δεν καταλαμβάνουν άσκοπο χώρο στο σκληρό σας δίσκο. Σχεδόν κάθε port παρέχεται επίσης και σαν προ-μεταγλωττισμένο (pre-compiled) "πακέτο (package)", το οποίο μπορεί να εγκατασταθεί με μια απλή εντολή (`pkg install`) για εκείνους που δεν επιθυμούν να μεταγλωττίζουν τα ports τους από τον πηγαίο κώδικα. Περισσότερες πληροφορίες για τα packages και τα ports μπορείτε να βρείτε στο Εγκατάσταση Εφαρμογών: Πακέτα και Ports.

3.5. Πρόσθετη Τεκμηρίωση

Όλες οι τρέχουσες εκδόσεις του FreeBSD παρέχουν επιλογή στο πρόγραμμα εγκατάστασης (είτε το sysinstall(8) ή το bsdinstall(8)) για την εγκατάσταση πρόσθετης τεκμηρίωσης στην τοποθεσία /usr/local/shared/doc/freebsd κατά την αρχική εγκατάσταση του συστήματος. Μπορείτε επίσης να εγκαταστήσετε την τεκμηρίωση οποιαδήποτε στιγμή αργότερα, χρησιμοποιώντας τα πακέτα όπως περιγράφεται στο “Χρήση Έτοιμων Πακέτων Τεκμηρίωσης”. Μπορείτε να δείτε την τοπικά εγκατεστημένη τεκμηρίωση χρησιμοποιώντας οποιοδήποτε πρόγραμμα φυλλομετρητή, στις

παρακάτω τοποθεσίες:

Το Εγχειρίδιο Χρήσης του FreeBSD

/usr/local/shared/doc/freebsd/handbook/index.html

Συχνές ερωτήσεις του FreeBSD (FAQ)

/usr/local/shared/doc/freebsd/faq/index.html

Μπορείτε επίσης να δείτε τα πρωτότυπα (και συχνά αναβαθμιζόμενα) αντίγραφα στο http://www.FreeBSD.org/.

Chapter 4. Εγκατάσταση του FreeBSD 9.x και Μεταγενέστερων Εκδόσεων

4.1. Σύνοψη

Το FreeBSD έρχεται με ένα μη-γραφικό αλλά εύκολο στη χρήση πρόγραμμα εγκατάστασης. Από το FreeBSD 9.0-RELEASE και μετά, χρησιμοποιείται το πρόγραμμα bsdinstall ενώ οι προηγούμενες εκδόσεις χρησιμοποιούν το sysinstall. Το κεφάλαιο αυτό περιγράφει τη χρήση του bsdinstall. Η χρήση του sysinstall περιγράφεται στο “Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων”.

Αφού διαβάσετε αυτό το κεφάλαιο, θα γνωρίζετε:

- Πως να δημιουργήσετε μέσα εγκατάστασης για το FreeBSD.
- Πως το FreeBSD υποδιαιρεί τους σκληρούς δίσκους και πως αναφέρεται σε αυτούς.
- Πως να εκκινήσετε το bsdinstall.
- Τις ερωτήσεις που θα σας κάνει το bsdinstall, τι σημαίνουν και πως να τις απαντήσετε.

Πριν διαβάσετε αυτό το κεφάλαιο θα πρέπει:

- Να διαβάσετε τη λίστα του υλικού που υποστηρίζεται από την έκδοση του FreeBSD που εγκαθιστάτε και να επαληθεύσετε ότι το υλικό του υπολογιστή σας υποστηρίζεται.

Σε γενικές γραμμές, αυτές οι οδηγίες εγκατάστασης αναφέρονται στην αρχιτεκτονική i386™ ("PC συμβατή"). Όπου χρειάζεται, γίνεται αναφορά και σε άλλες αρχιτεκτονικές. Πιθανόν να υπάρχουν μικρές διαφορές στο πρόγραμμα εγκατάστασης σε σχέση με το παρόν κείμενο και για το λόγο αυτό σας συνιστούμε να το χρησιμοποιήσετε ως γενικό οδηγό παρά σαν κυριολεκτικά ακριβείς οδηγίες.

4.2. Απαιτήσεις Υλικού

4.2.1. Ελάχιστες Απαιτήσεις Εγκατάστασης

Οι ελάχιστες απαιτήσεις για την εγκατάσταση του FreeBSD ποικίλουν ανάλογα με την έκδοση του λειτουργικού και την αρχιτεκτονική του υλικού που χρησιμοποιείται.

Στις επόμενες ενότητες θα σας παρουσιάσουμε μια σύνοψη αυτών των πληροφοριών. Ανάλογα με τη μέθοδο που θα χρησιμοποιήσετε για να εγκαταστήσετε το FreeBSD, μπορεί να χρειαστείτε ένα υποστηριζόμενο οδηγό CDROM και - σε κάποιες περιπτώσεις - μια κάρτα δικτύου. Τα θέματα αυτά καλύπτονται στο Προετοιμάστε τα Μέσα Εγκατάστασης.

4.2.1.1. FreeBSD/i386

Το FreeBSD/i386 απαιτεί 486 ή καλύτερο επεξεργαστή και τουλάχιστον 64 MB RAM. Για την ελάχιστη δυνατή εγκατάσταση απαιτείται 1.1 GB ελεύθερου χώρου στο σκληρό δίσκο.

Σε περιπτώσεις παλιών μηχανημάτων, τις περισσότερες φορές, η απόδοση του συστήματος βελτιώνεται περισσότερο με αύξηση της μνήμης RAM και του ελεύθερου χώρου στο δίσκο, παρά με ένα ταχύτερο επεξεργαστή.

4.2.1.2. FreeBSD/amd64

Υπάρχουν δύο κλάσεις επεξεργαστών ικανές να εκτελέσουν το FreeBSD/amd64. Η πρώτη είναι οι επεξεργαστές AMD64 που περιλαμβάνουν τους AMD Athlon™64, AMD Athlon™64-FX, AMD Opteron™ ή καλύτερους.

Η δεύτερη κλάση επεξεργαστών που μπορούν να εκτελέσουν το FreeBSD/amd64 περιλαμβάνει όσους χρησιμοποιούν την αρχιτεκτονική Intel® EM64T. Παραδείγματα των επεξεργαστών αυτών περιλαμβάνουν τις οικογένειες Intel® Core™ 2 Duo, Quad, Extreme processor, τη σειρά επεξεργαστών Intel® Xeon™ 3000, 5000 και 7000 καθώς και τους επεξεργαστές Intel® Core™ i3, i5 και i7.

Αν το μηχάνημα σας είναι βασισμένο σε nVidia nForce3 Pro-150, θα *πρέπει* να χρησιμοποιήσετε την κατάλληλη επιλογή στο BIOS για να απενεργοποιήσετε το IO APIC. Αν η επιλογή αυτή δεν υπάρχει, θα πρέπει να απενεργοποιήσετε αντί αυτού το ACPI. Υπάρχουν προβλήματα στο Pro-150 για τα οποία μέχρι στιγμής δεν έχει βρεθεί λύση που να τα παρακάμπτει.

4.2.1.3. FreeBSD/powerpc Apple® Macintosh®

Υποστηρίζονται όλοι οι νέοι υπολογιστές Apple® Macintosh® που διαθέτουν ενσωματωμένες USB. Υποστηρίζεται επίσης η λειτουργία SMP σε μηχανήματα με πολλαπλούς επεξεργαστές.

Ένας 32-bit πυρήνας μπορεί να χρησιμοποιήσει μόνο τα πρώτα 2 GB RAM. Το FireWire® δεν υποστηρίζεται στα Μπλε και Λευκά PowerMac G3.

4.2.1.4. FreeBSD/sparc64

Μπορείτε να δείτε τα συστήματα που υποστηρίζονται από το FreeBSD/sparc64 στο FreeBSD/sparc64 Project.

Θα χρειαστείτε ένα δίσκο για αποκλειστική χρήση από το FreeBSD/sparc64. Τη δεδομένη στιγμή, δεν είναι δυνατόν το FreeBSD/sparc64 να μοιράζεται τον ίδιο δίσκο με ένα άλλο λειτουργικό σύστημα.

4.2.2. Υποστηριζόμενο Υλικό

Στις Σημειώσεις Υλικού (Hardware Notes) μπορείτε να βρείτε πληροφορίες για τις αρχιτεκτονικές και τις συσκευές που υποστηρίζονται από μια επίσημη έκδοση του FreeBSD. Το αρχείο αυτό ονομάζεται συνήθως HARDWARE.TXT, και βρίσκεται στον κεντρικό κατάλογο του μέσου εγκατάστασης. Μπορείτε επίσης να βρείτε αντίγραφα αυτού του καταλόγου στη σελίδα Πληροφοριών Έκδοσης στο δικτυακό τόπο του FreeBSD.

4.3. Εργασίες πριν την Εγκατάσταση

4.3.1. Κρατήστε Αντίγραφα Ασφαλείας των Δεδομένων σας

Κρατήστε αντίγραφα ασφαλείας όλων των σημαντικών δεδομένων του υπολογιστή στον οποίο θα κάνετε εγκατάσταση του FreeBSD. Ελέγξτε τη σωστή λειτουργία των αντιγράφων ασφαλείας πριν συνεχίσετε. Το πρόγραμμα εγκατάστασης του FreeBSD θα ζητήσει επιβεβαίωση πριν κάνει οποιαδήποτε αλλαγή στο δίσκο σας, αλλά από τη στιγμή που αυτή η διαδικασία ξεκινήσει, δεν υπάρχει δυνατότητα επιστροφής.

4.3.2. Αποφασίστε που θα Εγκαταστήσετε το FreeBSD

Αν το FreeBSD πρόκειται να είναι το μοναδικό λειτουργικό σύστημα του υπολογιστή και σκοπεύετε να διαθέσετε σε αυτό ολόκληρο το χώρο του σκληρού σας δίσκου, μπορείτε να παραλείψετε το υπόλοιπο αυτής της ενότητας. Αν ωστόσο θέλετε να συνυπάρχει το FreeBSD με άλλα λειτουργικά συστήματα, είναι χρήσιμο να κατανοείτε γενικά τον τρόπο διάταξης των δεδομένων στο δίσκο.

4.3.2.1. Κατατμήσεις Δίσκων για τις Αρχιτεκτονικές FreeBSD/i386 και FreeBSD/amd64

Οι σκληροί δίσκοι μπορούν να χωριστούν σε διακριτά τμήματα. Τα τμήματα αυτά ονομάζονται *κατατμήσεις (partitions)*.

Υπάρχουν δύο τρόποι για να χωριστεί ένας δίσκος σε κατατμήσεις. Ο παραδοσιακός τρόπος χρησιμοποιεί το *Master Boot Record (Βασική Εγγραφή Εκκίνησης)* ή MBR, ένα πίνακα κατατμήσεων ικανό να αποθηκεύσει ως τέσσερις *πρωτεύουσες κατατμήσεις (primary partitions)*. (Για ιστορικούς λόγους, το FreeBSD ονομάζει τις πρωτεύουσες κατατμήσεις *slices ή φέτες*.) Το όριο των τεσσάρων κατατμήσεων είναι πολύ περιοριστικό για μεγάλους δίσκους, έτσι μια από αυτές τις κατατμήσεις μπορεί να μετατραπεί σε *εκτεταμένη κατάτμηση (extended partition)*. Μέσα στην εκτεταμένη κατάτμηση μπορούν να δημιουργηθούν πολλαπλές *λογικές κατατμήσεις (logical partitions)*. Αυτό ακούγεται κάπως παράξενο, και μάλλον είναι.

Ο *Πίνακας Κατατμήσεων GUID (GUID Partition Table)* ή GPT, αποτελεί μια νέα και απλούστερη μέθοδος κατάτμησης ενός δίσκου. Το GPT είναι πολύ πιο βολικό από τον παραδοσιακό πίνακα κατατμήσεων MBR. Οι συνήθεις υλοποιήσεις του GPT επιτρέπουν ως και 128 κατατμήσεις ανά δίσκο, εξαλείφοντας έτσι την ανάγκη για άβολες λύσεις όπως οι λογικές κατατμήσεις.

Κάποια παλιότερα λειτουργικά συστήματα όπως τα Windows® XP δεν είναι συμβατά με το σύστημα κατατμήσεων GPT. Αν το FreeBSD πρόκειται να εγκατασταθεί σε ένα δίσκο από κοινού με ένα τέτοιο λειτουργικό, θα πρέπει να χρησιμοποιήσετε το σύστημα MBR.

Ο τυπικός φορτωτής εκκίνησης (boot loader) του FreeBSD χρειάζεται είτε μια πρωτεύουσα είτε μια GPT κατάτμηση. (Δείτε το Η Διαδικασία Εκκίνησης του FreeBSD για περισσότερες πληροφορίες σχετικά με τη διαδικασία εκκίνησης του FreeBSD.) Αν όλες οι πρωτεύουσες ή GPT κατατμήσεις είναι ήδη σε χρήση, θα πρέπει να ελευθερώσετε μία για χρήση με το FreeBSD.

Η ελάχιστη εγκατάσταση του FreeBSD καταλαμβάνει μόνο περίπου 1 GB χώρο στο δίσκο. Πρόκειται όμως για την *απόλυτα* ελάχιστη εγκατάσταση η οποία δεν αφήνει σχεδόν καθόλου ελεύθερο χώρο. Μια πιο ρεαλιστική ελάχιστη εγκατάσταση καταλαμβάνει περίπου 3 GB χωρίς γραφικό περιβάλλον και περίπου 5 GB με χρήση κάποιου γραφικού περιβάλλοντος. Η εγκατάσταση λογισμικού τρίτων κατασκευαστών απαιτεί ακόμα περισσότερο χώρο στο δίσκο.

Υπάρχει πληθώρα ελεύθερων και εμπορικών εργαλείων αναδιανομής χώρου κατατμήσεων. Το GParted Live είναι ένα δωρεάν Live CD το οποίο περιλαμβάνει τον επεξεργαστή κατατμήσεων GParted. Το GParted περιλαμβάνεται επίσης σε πολλές άλλες Live διανομές Linux.

Οι εφαρμογές που διαχειρίζονται κατατμήσεις σκληρών δίσκων μπορούν να καταστρέψουν τα δεδομένα σας. Πάρτε πλήρη αντίγραφα ασφαλείας και επιβεβαιώστε την ορθή λειτουργία τους πριν ξεκινήσετε την τροποποίηση των κατατμήσεων του δίσκου σας.

Η αλλαγή μεγέθους κατατμήσεων των Microsoft® Vista ενδέχεται να είναι δύσκολη. Είναι χρήσιμο να έχετε διαθέσιμο ένα DVD εγκατάστασης των Vista πριν ξεκινήσετε μια τέτοια διαδικασία.

Παράδειγμα 1. Χρησιμοποιώντας μια Υπάρχουσα Κατάτμηση

Ένας υπολογιστής Windows® διαθέτει ένα μοναδικό δίσκο 40 GB ο οποίος έχει χωριστεί σε δύο κατατμήσεις των 20 GB. Στα Windows® ονομάζονται C: και D:. Η κατάτμηση C: περιέχει 10 GB δεδομένων, ενώ η κατάτμηση D: 5 GB.

Η μετακίνηση των δεδομένων από τον D: στο C: ελευθερώνει τη δεύτερη κατάτμηση ώστε να μπορεί να χρησιμοποιηθεί από το FreeBSD.

Παράδειγμα 2. Συρρικνώνοντας μια Υπάρχουσα Κατάτμηση

Ένας υπολογιστής Windows® έχει ένα μοναδικό σκληρό δίσκο 40 GB και μια μεγάλη κατάτμηση που τον καταλαμβάνει εξ' ολοκλήρου. Τα Windows® δείχνουν αυτή την κατάτμηση των 40 GB ως ένα μοναδικό οδηγό C:. Τη δεδομένη στιγμή χρησιμοποιούνται 15 GB χώρου. Σκοπός είναι να καταλήξουμε με μια κατάτμηση των 20 GB για τα Windows® και άλλα 20 GB για το FreeBSD.

Υπάρχουν δύο τρόποι για να γίνει αυτό:

1. Κρατήστε αντίγραφο των δεδομένων που έχετε δημιουργήσει στα Windows®. Έπειτα επανεγκαταστήστε τα Windows® δημιουργώντας μια κατάτμηση μεγέθους 20 GB κατά την διαδικασία εγκατάστασης.
2. Χρησιμοποιήστε κάποιο εργαλείο αλλαγής μεγέθους κατατμήσεων όπως το GParted για να συρρικνώσετε την κατάτμηση των Windows® και να δημιουργήσετε μια νέα κατάτμηση για το FreeBSD στον ελεύθερο χώρο.

Η εγκατάσταση διαφορετικών λειτουργικών συστημάτων σε άλλες κατατμήσεις, επιτρέπει την εκτέλεση ενός από αυτά σε μια δεδομένη χρονική στιγμή. Μια εναλλακτική μέθοδος που επιτρέπει την ταυτόχρονη εκτέλεση πολλών λειτουργικών περιγράφεται στο Εικονικοποίηση.

4.3.3. Συλλέξτε Πληροφορίες για το Δίκτυο

Κάποιες μέθοδοι εγκατάστασης του FreeBSD χρειάζονται μια σύνδεση δικτύου για να κατεβάσουν αρχεία. Για να συνδεθείτε με ένα δίκτυο Ethernet (ή μέσω καλωδιακού ή DSL modem με διεπαφή Ethernet), το πρόγραμμα εγκατάστασης θα σας ζητήσει πληροφορίες σχετικά με το δίκτυο σας.

Συχνά, γίνεται χρήση του *DHCP* ώστε οι ρυθμίσεις του δικτύου να γίνονται αυτόματα. Αν δεν διαθέτετε DHCP, θα πρέπει να βρείτε τις παρακάτω πληροφορίες από τον τοπικό σας διαχειριστή δικτύου ή τον παροχέα των υπηρεσιών σας:

1. Διεύθυνση IP
2. Μάσκα Υποδικτύου
3. Διεύθυνση IP προεπιλεγμένου δρομολογητή
4. Όνομα Τομέα για το τοπικό δίκτυο
5. Διευθύνσεις IP των διακομιστών DNS

4.3.4. Ελέγξτε για Παροράματα (Errata) στο FreeBSD

Αν και το FreeBSD Project πασχίζει για να εξασφαλίσει ότι κάθε νέα έκδοση του FreeBSD θα είναι όσο πιο σταθερή γίνεται, ορισμένες φορές στη διαδικασία αυτή εισέρχονται λάθη. Σε πολύ σπάνιες περιπτώσεις, τα λάθη αυτά επηρεάζουν τη διαδικασία εγκατάστασης. Καθώς τα προβλήματα αυτά γίνονται αντιληπτά και επιδιορθώνονται, σημειώνονται στα Παροράματα του FreeBSD στη δικτυακή τοποθεσία του FreeBSD. Ελέγξτε τα παροράματα πριν ξεκινήσετε την εγκατάσταση, για να βεβαιωθείτε ότι δεν υπάρχουν προβλήματα που μπορούν να επηρεάσουν τη διαδικασία.

Μπορείτε να βρείτε πληροφορίες και παροράματα για όλες τις εκδόσεις στη σελίδα πληροφοριών έκδοσης στην δικτυακή τοποθεσία του FreeBSD.

4.3.5. Προετοιμάστε τα Μέσα Εγκατάστασης

Η εγκατάσταση του FreeBSD ξεκινάει με την εκκίνηση του υπολογιστή με τη χρήση ενός FreeBSD CD, DVD ή μνήμης USB. Το πρόγραμμα εγκατάστασης δεν μπορεί να εκτελεστεί μέσα από κάποιο άλλο λειτουργικό σύστημα.

Εκτός από τα τυποποιημένα μέσα εγκατάστασης που περιέχουν όλα τα απαραίτητα αρχεία εγκατάστασης του FreeBSD, διατίθεται επίσης και η εκδοχή *bootonly*. Αυτό το μέσο εγκατάστασης δεν περιέχει τα απαραίτητα αρχεία, αλλά τα κατεβάζει από το δίκτυο κατά τη διάρκεια της εγκατάστασης. Κατά συνέπεια, το συγκεκριμένο CD είναι αρκετά μικρότερο σε μέγεθος ενώ και το απαιτούμενο εύρος ζώνης του δικτύου περιορίζεται καθώς κατεβαίνουν μόνο τα αρχεία που απαιτούνται.

Μπορείτε να βρείτε έτοιμα μέσα εγκατάστασης για το FreeBSD στην δικτυακή τοποθεσία του FreeBSD.. Κατεβάστε επίσης το αρχείο CHECKSUM.SHA256 από τον ίδιο κατάλογο που περιέχει και το αρχείο εγκατάστασης και χρησιμοποιήστε το για να ελέγξετε την ακεραιότητα του αρχείου εγκατάστασης υπολογίζοντας το *Άθροισμα Ελέγχου (checksum)*. Το FreeBSD διαθέτει το sha256(1) για αυτό το σκοπό και θα βρείτε αντίστοιχα προγράμματα και σε άλλα λειτουργικά συστήματα. Επαληθεύστε το άθροισμα ελέγχου σύμφωνα με αυτό που αναγράφεται στο αρχείο CHECKSUM.SHA256. Τα αθροίσματα πρέπει να είναι ίδια. Αν δεν είναι, το αρχείο εγκατάστασης αλλοιώθηκε κατά το κατέβασμα και είναι άχρηστο.

Αν διαθέτετε ήδη ένα CDROM, DVD ή USB οδηγό εγκατάστασης FreeBSD, μπορείτε να παραλείψετε αυτή την ενότητα.

Τα CD και DVD αρχεία ISO του FreeBSD είναι εκκινήσιμα. Χρειάζεστε μόνο ένα από αυτά για την εγκατάσταση. Γράψτε το αρχείο ISO σε ένα CD ή DVD χρησιμοποιώντας τα αντίστοιχα προγράμματα εγγραφής που διαθέτει το τρέχον λειτουργικό σας σύστημα. Στο FreeBSD, η εγγραφή μπορείτε να γίνει με το πρόγραμμα cdrecord(1) από το port sysutils/cdrtools που μπορείτε να εγκαταστήσετε από τη Συλλογή των Ports.

Για να δημιουργήσετε μια εκκινήσιμη μνήμη Flash (USB), ακολουθήστε τα παρακάτω βήματα:

1. Ανακτήστε το Αρχείο ISO για τη Μνήμη Flash

   Για το FreeBSD 9.0-RELEASE και μεταγενέστερες εκδόσεις, μπορείτε να κατεβάσετε το αντίστοιχο αρχείο από τον κατάλογο ISO-IMAGES/ στην τοποθεσία `ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/arch/arch/ISO-IMAGES/version/FreeBSD-version-RELEASE-arch-memstick.img`. Αντικαταστήστε το *arch* και το *version* με την αρχιτεκτονική και την έκδοση που θέλετε να εγκαταστήσετε. Για παράδειγμα, το αρχείο για το FreeBSD/i386 9.0-RELEASE βρίσκεται στη θέση ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/i386/ISO-IMAGES/9.0/FreeBSD-9.0-RELEASE-i386-memstick.img.

   > Ο κατάλογος είναι διαφορετικός για το FreeBSD 8.*X* και προηγούμενες εκδόσεις. Για περισσότερες πληροφορίες σχετικά με το κατέβασμα και την εγκατάσταση του FreeBSD 8.*X* και προηγούμενων εκδόσεων, δείτε το Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων.

   Το αρχείο για τη μνήμη Flash έχει επέκταση .img. Ο κατάλογος ISO-IMAGES/ περιέχει πλήθος από διαφορετικά αρχεία. Θα πρέπει να κατεβάσετε το κατάλληλο ανάλογα με την έκδοση του FreeBSD και το υλικό του υπολογιστή που πρόκειται να χρησιμοποιηθεί.

   > Πριν προχωρήσετε, *αντιγράψτε* τυχόν δεδομένα που έχετε ήδη στη μνήμη USB, καθώς η παρακάτω διαδικασία θα τα *διαγράψει*.

2. Γράψτε το Αρχείο στη Μνήμη USB

Procedure: Εγγραφή του Αρχείου με Χρήση του FreeBSD

> Το παρακάτω παράδειγμα δείχνει τη συσκευή /dev/da0 ως τον προορισμό εγγραφής του αρχείου. Θα πρέπει να είστε πολύ προσεκτικοί και να βεβαιωθείτε για το όνομα της συσκευής που χρησιμοποιείτε, διαφορετικά ενδέχεται να διαγράψετε δεδομένα που χρειάζεστε.

1. Εγγραφή του Αρχείου με την dd(1)

   Το αρχείο .img*δεν* είναι ένα συνηθισμένο αρχείο. Είναι ένα αρχείο *εικόνας (image)* με όλο το περιεχόμενο που χρειάζεται η μνήμη USB. *Δεν μπορείτε* να το αντιγράψετε ως ένα κανονικό αρχείο, θα χρειαστεί να το γράψετε απευθείας στη συσκευή προορισμού

χρησιμοποιώντας την εντολή dd(1):

```
# dd if=FreeBSD-9.0-RELEASE-i386-memstick.img of=/dev/da0 bs=64k
```

Procedure: Εγγραφή του Αρχείου Μέσω Windows®

> Βεβαιωθείτε ότι χρησιμοποιείτε το σωστό όνομα οδηγού για την μνήμη USB, διαφορετικά μπορεί να προκληθεί απώλεια δεδομένων.

1. Ανάκτηση του Προγράμματος Image Writer για Windows®

   Το Image Writer για Windows® είναι μια δωρεάν εφαρμογή που μπορεί να γράψει σωστά ένα αρχείο image σε μια μνήμη USB. Μπορείτε να το κατεβάσετε από την τοποθεσία https://launchpad.net/win32-image-writer/ και να το αποσυμπιέσετε σε ένα φάκελο.

2. Εγγραφή του Αρχείου με το Image Writer

   Κάντε διπλό κλικ στο εικονίδιο Win32DiskImager για να ξεκινήσετε το πρόγραμμα. Βεβαιωθείτε ότι το γράμμα του οδηγού που φαίνεται στην επιλογή `Device` αντιστοιχεί στη μνήμη USB. Κάντε κλικ στο εικονίδιο με το φάκελο και επιλέξτε το αρχείο εικόνας που θα γραφεί στη μνήμη USB. Κάντε κλικ στο **[Save]** για να αποδεχθείτε το όνομα του αρχείου εικόνας. Βεβαιωθείτε ότι οι παραπάνω ενέργειες είναι σωστές και ότι δεν υπάρχουν ανοικτά παράθυρα στο σύστημα σας που να απεικονίζουν φακέλους της μνήμης USB. Τέλος, κάντε κλικ στο **[Write]** για να γράψετε το αρχείο εικόνας στη μνήμη USB.

Δεν υποστηρίζεται πλέον η εγκατάσταση από δισκέτες

Είστε πλέον έτοιμοι να ξεκινήσετε την εγκατάσταση του FreeBSD.

4.4. Ξεκινώντας την Εγκατάσταση

Από προεπιλογή, η εγκατάσταση δεν θα κάνει αλλαγές στους δίσκους σας μέχρι να δείτε το παρακάτω μήνυμα:

```
Your changes will now be written to disk.  If you
have chosen to overwrite existing data, it will
be PERMANENTLY ERASED. Are you sure you want to
commit your changes?
```

Μπορείτε να εγκαταλείψετε την εγκατάσταση οποιαδήποτε στιγμή πριν από την

> παραπάνω προειδοποίηση, χωρίς να έχουν γίνει αλλαγές στα περιεχόμενα του δίσκου σας. Αν ανησυχείτε ότι ενδεχομένως έχετε κάνει κάτι λάθος, μπορείτε απλά να σβήσετε τον υπολογιστή σας πριν από αυτό το σημείο και δεν θα γίνει καμιά ζημιά.

4.4.1. Εκκίνηση

4.4.1.1. Εκκίνηση στις Αρχιτεκτονικές i386™ και amd64

1. Αν προετοιμάσατε μια "εκκινήσιμη" μνήμη USB όπως περιγράφεται στο Προετοιμάστε τα Μέσα Εγκατάστασης, τοποθετήστε τη μνήμη στην υποδοχή του υπολογιστή σας πριν τον ενεργοποιήσετε.

   Αν πρόκειται να εκκινήσετε από το CDROM, θα χρειαστεί να ενεργοποιήσετε τον υπολογιστή σας και να εισάγετε το CDROM όσο πιο γρήγορα γίνεται.

2. Ρυθμίστε το μηχάνημα σας να ξεκινάει είτε από το CDROM είτε από την USB, ανάλογα με το μέσο εγκατάστασης που πρόκειται να χρησιμοποιήσετε. Γενικά, αυτό επιτυγχάνεται αλλάζοντας τη σχετική ρύθμιση στο BIOS. Τα περισσότερα συστήματα επιτρέπουν επίσης την επιλογή μιας συσκευής εκκίνησης καθώς ξεκινούν, τυπικά με τα πλήκτρα `F10`, `F11`, `F12`, ή `Escape`.
3. Αν ο υπολογιστής σας ξεκινήσει όπως συνήθως και φορτώσει το ήδη υπάρχον λειτουργικό σύστημα, μπορεί να συμβαίνει κάτι από τα παρακάτω:
   a. Δεν τοποθετήσατε το CD ή DVD αρκετά νωρίς κατά την εκκίνηση. Αφήστε το μέσο στον οδηγό και δοκιμάστε να επανεκκινήσετε τον υπολογιστή σας.
   b. Οι αλλαγές ρυθμίσεων που κάνατε στο BIOS δεν λειτούργησαν σωστά. Θα πρέπει να ξαναδοκιμάσετε μέχρι να πετύχετε τις σωστές ρυθμίσεις.
   c. Το BIOS της μητρικής σας δεν υποστηρίζει εκκίνηση από το μέσο που έχετε επιλέξει. Μπορείτε να χρησιμοποιήσετε τον Plop Boot Manager για να εκκινήσετε παλιά μηχανήματα από CD ή USB.
4. Θα αρχίσει η εκκίνηση του FreeBSD. Αν ξεκινάτε από CDROM, θα δείτε μια οθόνη σαν την παρακάτω (έχουμε παραλείψει τις πληροφορίες έκδοσης):

```
Booting from CD-ROM...
645MB medium detected
CD Loader 1.2

Building the boot loader arguments
Looking up /BOOT/LOADER... Found
Relocating the loader and the BTX
Starting the BTX loader

BTX loader 1.00 BTX version is 1.02
Consoles: internal video/keyboard
BIOS CD is cd0
BIOS drive C: is disk0
BIOS drive D: is disk1
BIOS 636kB/261056kB available memory
```

```
FreeBSD/i386 bootstrap loader, Revision 1.1

Loading /boot/defaults/loader.conf
/boot/kernel/kernel text=0x64daa0 data=0xa4e80+0xa9e40 syms
=[0x4+0x6cac0+0x4+0x88e9d]
\
```

5. Εμφανίζεται η οθόνη του φορτωτή εκκίνησης του FreeBSD:

Σχήμα 1. Μενού Φορτωτή Εκκίνησης του FreeBSD

Περιμένετε δέκα δευτερόλεπτα, ή πιέστε `Enter`.

4.4.1.2. Εκκίνηση στον Macintosh® PowerPC®

Στα περισσότερα μηχανήματα, μπορείτε να κρατήσετε πιεσμένο το πλήκτρο `C` κατά την εκκίνηση και θα ξεκινήσετε από το CD. Σε διαφορετική περίπτωση, κρατήστε πιεσμένα τα πλήκτρα `Command` + `Option` + `O` + `F`, ή `Windows` + `Alt` + `O` + `F` αν χρησιμοποιείτε πληκτρολόγιο που δεν είναι Apple®. Στην προτροπή `0 >` γράψτε:

```
boot cd:,\ppc\loader cd:0
```

Σε μηχανήματα Xserve χωρίς πληκτρολόγιο, δείτε την σελίδα τεχνικής υποστήριξης της Apple® για πληροφορίες εκκίνησης στο Open Firmware.

4.4.1.3. Εκκίνηση στον sparc64

Τα περισσότερα συστήματα sparc64 είναι ρυθμισμένα να εκκινούν αυτόματα από το σκληρό δίσκο. Για να εγκαταστήσετε το FreeBSD, θα πρέπει να εκκινήσετε από το δίκτυο ή από ένα CDROM. Θα χρειαστεί να εισέλθετε στις ρυθμίσεις της PROM (OpenFirmware).

Για να γίνει αυτό, επανεκκινήστε το σύστημα και περιμένετε μέχρι να εμφανιστεί το μήνυμα εκκίνησης. Το ακριβές μήνυμα εξαρτάται από το μοντέλο, αλλά γενικά θα δείχνει όπως το παρακάτω:

```
Sun Blade 100 (UltraSPARC-IIe), Keyboard Present
Copyright 1998-2001 Sun Microsystems, Inc.  All rights reserved.
OpenBoot 4.2, 128 MB memory installed, Serial #51090132.
Ethernet address 0:3:ba:b:92:d4, Host ID: 830b92d4.
```

Αν μετά από αυτό το σημείο το σύστημα σας συνεχίζει με εκκίνηση από το σκληρό δίσκο, θα πρέπει να πιέσετε `L1` + `A` ή `Stop` + `A` στο πληκτρολόγιο, ή να στείλετε σήμα `BREAK` μέσω της σειριακής κονσόλας (χρησιμοποιώντας π.χ. το `~#` στο tip(1) ή cu(1)) για να βγείτε στην προτροπή της PROM η οποία μοιάζει με την παρακάτω:

```
ok     ①
ok {0} ②
```

① Αυτή η προτροπή φαίνεται σε συστήματα με μόνο μία CPU.

② Αυτή η προτροπή φαίνεται σε συστήματα SMP. Το ψηφίο δείχνει τον αριθμό της ενεργής CPU.

Στο σημείο αυτό, τοποθετήστε το CDROM στον οδηγό και στην προτροπή της PROM γράψτε `boot cdrom`.

4.4.2. Επισκόπηση των Αποτελεσμάτων Ανίχνευσης Συσκευών

Οι τελευταίες εκατοντάδες γραμμές που πέρασαν από την οθόνη σας αποθηκεύονται και μπορείτε να τις ξαναδείτε.

Για να δείτε τα περιεχόμενα της προσωρινής μνήμης (buffer) πιέστε `Scroll Lock`. Με τον τρόπο αυτό ενεργοποιείται η κύλιση της οθόνης. Μπορείτε έπειτα να χρησιμοποιήσετε τα πλήκτρα με τα βελάκια ή τα `PageUp` και `PageDown` για να δείτε τα αποτελέσματα. Πιέστε ξανά το `Scroll Lock` για να σταματήσετε την κύλιση.

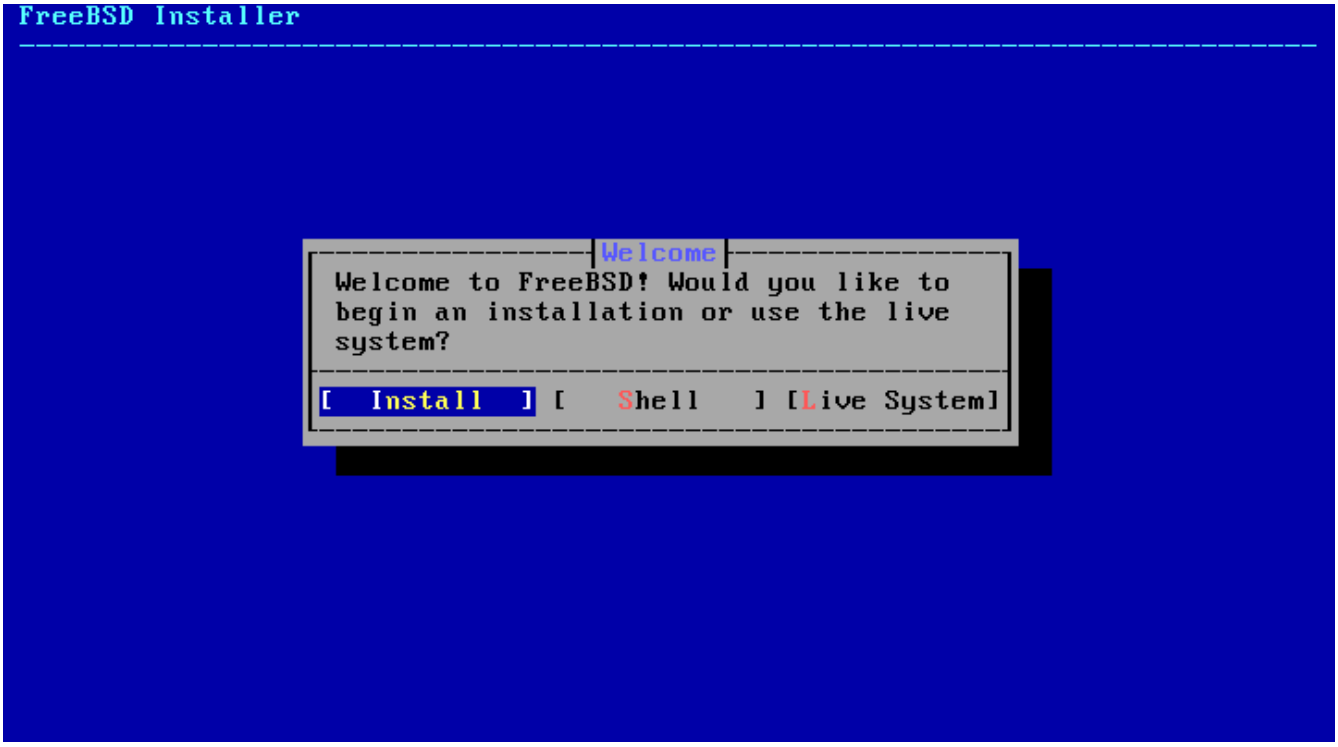
Κάντε το αυτό τώρα, για να ξαναδείτε το κείμενο που κύλησε εκτός οθόνης καθώς ο πυρήνας εκτελούσε την ανίχνευση συσκευών. Θα δείτε κείμενο αντίστοιχο με το Τυπικά Αποτελέσματα Ανίχνευσης Συσκευών, αν και θα υπάρχουν διαφορές ανάλογα με τις συσκευές που διαθέτει ο υπολογιστής σας.

Τυπικά Αποτελέσματα Ανίχνευσης Συσκευών

Ελέγξτε προσεκτικά τα αποτελέσματα της ανίχνευσης συσκευών για να βεβαιωθείτε ότι το FreeBSD βρήκε όλες τις συσκευές που αναμένατε. Αν κάποια συσκευή δεν βρέθηκε, δεν θα φαίνεται στην παραπάνω λίστα. Τα Αρθρώματα Πυρήνα σας επιτρέπουν να προσθέσετε υποστήριξη για συσκευές που δεν υπάρχουν στον πυρήνα GENERIC.

Μετά τη διαδικασία ανίχνευσης συσκευών θα δείτε το Επιλογή Τρόπου Λειτουργίας Μέσου Εγκατάστασης. Το μέσο εγκατάστασης μπορεί να χρησιμοποιηθεί με τρεις τρόπους: για να εγκαταστήσετε το FreeBSD, ως "live CD" ή απλά για να αποκτήσετε πρόσβαση σε ένα κέλυφος του

FreeBSD. Χρησιμοποιήστε τα βελάκια για να κάνετε μια επιλογή και το `Enter` για να την επιβεβαιώσετε.



Σχήμα 2. Επιλογή Τρόπου Λειτουργίας Μέσου Εγκατάστασης

Επιλέξτε **[Install]** για να ξεκινήσετε το πρόγραμμα εγκατάστασης.

4.5. Εισαγωγή στο bsdinstall

Το bsdinstall είναι μια εφαρμογή εγκατάστασης για το FreeBSD που βασίζεται σε περιβάλλον κειμένου. Γράφτηκε από τον Nathan Whitehorn <nwhitehorn@FreeBSD.org> και χρησιμοποιήθηκε πρώτη φορά το 2011 στο FreeBSD 9.0.

Η εφαρμογή pc-sysinstall του Kris Moore <kmoore@FreeBSD.org> συμπεριλαμβάνεται με το PC-BSD και μπορεί επίσης να χρησιμοποιηθεί για την εγκατάσταση του FreeBSD. Αν και μερικές φορές συγχέεται με το bsdinstall οι δύο αυτές εφαρμογές δεν σχετίζονται.

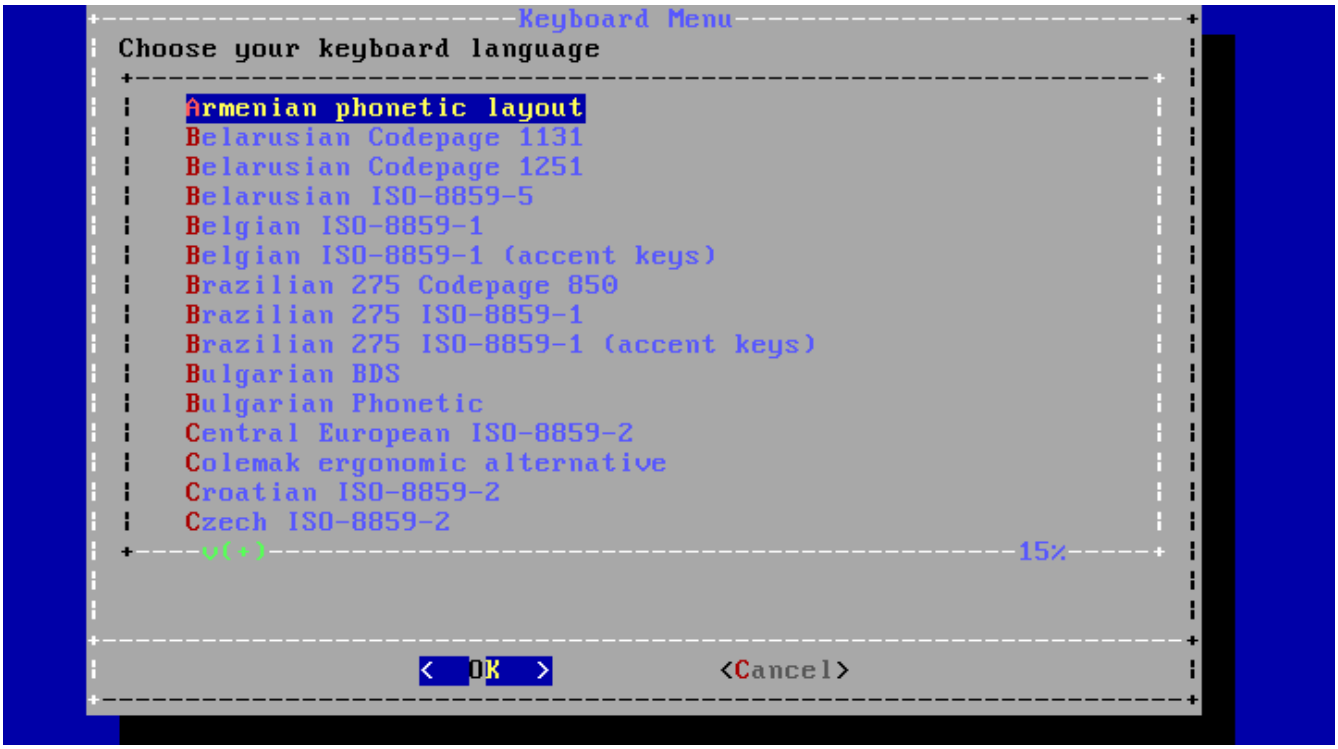
Το σύστημα μενού του bsdinstall ελέγχεται μέσω των πλήκτρων με τα βελάκια και τα πλήκτρα `Enter`, `Tab`, `Space` και μερικά ακόμα.

4.5.1. Επιλογές στο Μενού Keymap

Ανάλογα με το είδος της κονσόλας που χρησιμοποιείτε, το bsdinstall ίσως σας ρωτήσει αν επιθυμείτε να επιλέξετε μια διάταξη πληκτρολογίου διαφορετική από την προεπιλεγμένη.

Σχήμα 3. Επιλογή Διάταξης Πληκτρολογίου

Αν επιλέξετε **[YES]** θα εμφανιστεί η οθόνη επιλογής που φαίνεται παρακάτω. Σε διαφορετική περίπτωση, η οθόνη αυτή δεν θα εμφανιστεί και θα χρησιμοποιηθεί η προεπιλεγμένη διάταξη πληκτρολογίου.



Σχήμα 4. Μενού Επιλογής Διάταξης Πληκτρολογίου

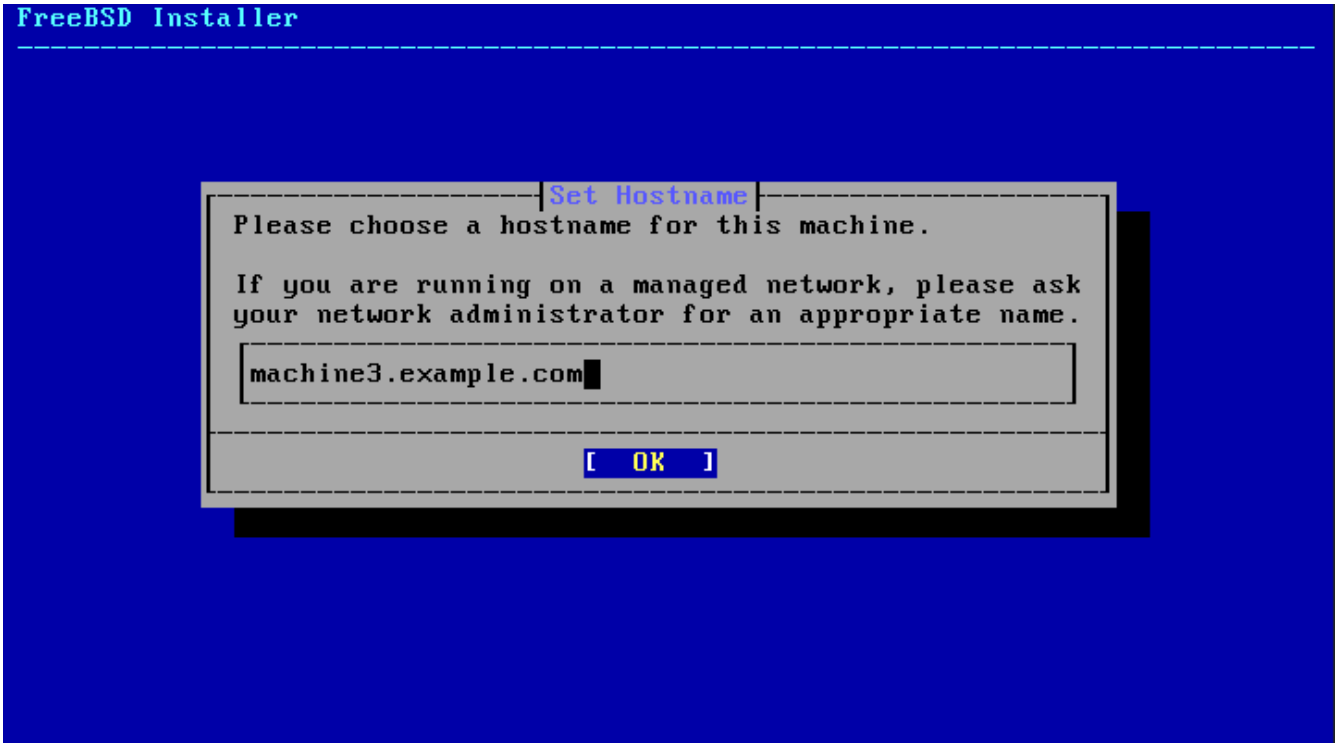
Επιλέξτε την διάταξη πληκτρολογίου που είναι πιο κοντά στο πληκτρολόγιο που διαθέτετε, χρησιμοποιώντας τα πάνω και κάτω βελάκια και επιβεβαιώνοντας με το `Enter`.

Αν πιέσετε `Esc` θα χρησιμοποιηθεί η προεπιλεγμένη διάταξη. Αν η διάταξη του τρέχοντος πληκτρολογίου δεν είναι προφανής, μια ασφαλής επιλογή είναι το

United States of America ISO-8859-1.

4.5.2. Καθορισμός Ονόματος Υπολογιστή (hostname)

Στο επόμενο βήμα, το bsdinstall θα σας ρωτήσει για το όνομα υπολογιστή (hostname) το οποίο θα δοθεί στο νέο σύστημα.

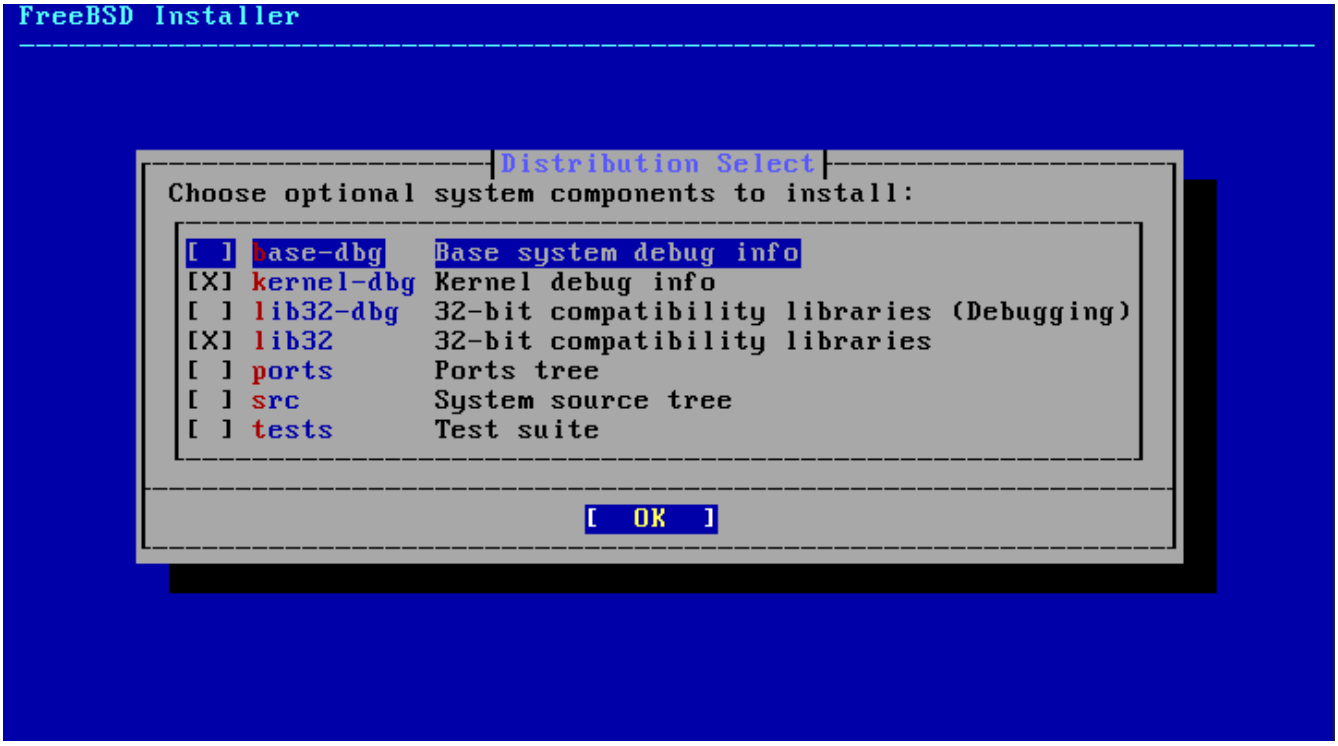


Σχήμα 5. Καθορισμός Ονόματος Υπολογιστή

Το όνομα που θα δώσετε πρέπει να περιλαμβάνει και τον τομέα (fully-qualified) όπως για παράδειγμα `machine3.example.com`

4.5.3. Επιλογή Στοιχείων Εγκατάστασης

Στο επόμενο βήμα, το bsdinstall θα σας καλέσει να επιλέξετε ποια προαιρετικά στοιχεία του λειτουργικού επιθυμείτε να εγκαταστήσετε.



Σχήμα 6. Επιλογή Στοιχείων Εγκατάστασης

Η επιλογή των στοιχείων εγκατάστασης εξαρτάται κυρίως από την χρήση που θα έχει το σύστημα και το διαθέσιμο ελεύθερο χώρο στο δίσκο. Ο πυρήνας και τα βασικά προγράμματα του FreeBSD (γνωστά και ως "base system" ή βασικό σύστημα) εγκαθίστανται υποχρεωτικά.

Ανάλογα με το είδος της εγκατάστασης, κάποια από τα παρακάτω στοιχεία μπορεί να μην εμφανιστούν.

Προαιρετικά Στοιχεία

- `doc` - Επιπρόσθετη τεκμηρίωση, κυρίως ιστορικής σημασίας. Η τεκμηρίωση που παρέχεται από την Ομάδα Τεκμηρίωσης του FreeBSD εγκαθίσταται χωριστά σε επόμενο στάδιο.
- `games` - Κάποια παραδοσιακά BSD παιχνίδια που περιλαμβάνουν τα fortune, rot13 και άλλα.
- `lib32` - Βιβλιοθήκες συμβατότητας για εκτέλεση εφαρμογών 32-bit σε 64-bit εκδόσεις του FreeBSD.
- `ports` - Η Συλλογή των Ports του FreeBSD.

  Η Συλλογή των Ports αποτελεί ένα εύκολο και βολικό τρόπο εγκατάστασης λογισμικού. Η Συλλογή των Ports δεν περιέχει τον πηγαίο κώδικα που απαιτείται για τη μεταγλώττιση του λογισμικού. Πρόκειται στην πραγματικότητα για μια συλλογή αρχείων που αυτοματοποιεί τη μεταφόρτωση, μεταγλώττιση και εγκατάσταση λογισμικού τρίτων κατασκευαστών. Το Εγκατάσταση Εφαρμογών: Πακέτα και Ports αναλύει τον τρόπο χρήσης της Συλλογής των Ports.

Το πρόγραμμα εγκατάστασης δεν ελέγχει για να δει αν διαθέτετε αρκετό ελεύθερο χώρο στο δίσκο. Επιλέξτε αυτό το στοιχείο μόνο αν έχετε αρκετό χώρο. Από το FreeBSD 9.0 και μετά, η Συλλογή των Ports καταλαμβάνει περίπου 3 GB χώρο στο δίσκο. Μπορείτε με βεβαιότητα να θεωρήσετε ότι ο χώρος αυτός θα είναι ακόμα μεγαλύτερος στις νεώτερες εκδόσεις του FreeBSD.

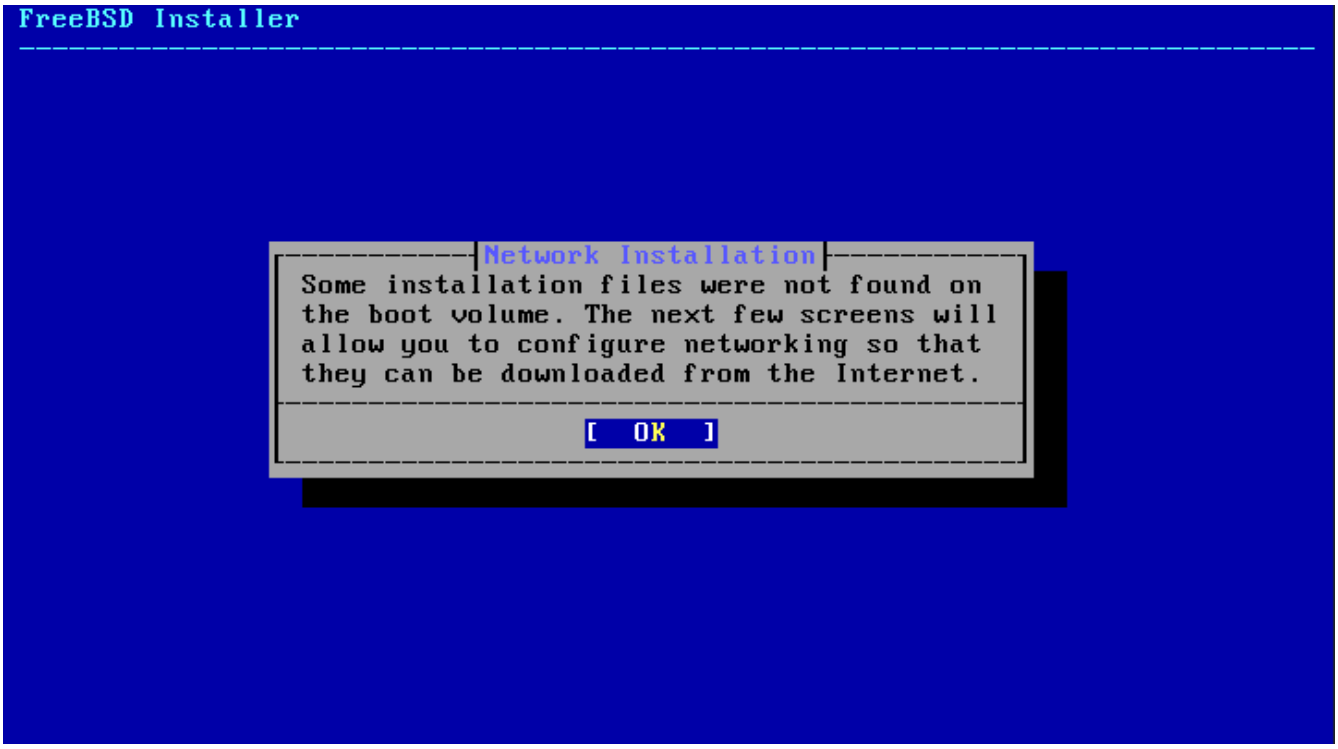
- `src` - Ο Πηγαίος Κώδικας του Συστήματος.

  Το FreeBSD έρχεται με πλήρη πηγαίο κώδικα, τόσο για τον πυρήνα όσο και για τα βασικά προγράμματα. Αν και ο πηγαίος κώδικας δεν απαιτείται για την πλειονότητα των εφαρμογών, ίσως να τον χρειαστείτε για τη μεταγλώττιση συγκεκριμένων προγραμμάτων που παρέχονται ως πηγαίος κώδικας (π.χ. οδηγούς συσκευών ή αρθρώματα πυρήνα), ή για εργασίες ανάπτυξης του ίδιου του FreeBSD.

  Το πλήρες δέντρο του πηγαίου κώδικα καταλαμβάνει 1 GB χώρου στο δίσκο, ενώ μια πλήρης μεταγλώττιση όλου του FreeBSD απαιτεί επιπλέον 5 GB χώρου.

4.6. Εγκατάσταση από το Δίκτυο

Το μέσο εγκατάστασης *bootonly* δεν διαθέτει αντίγραφα των αρχείων εγκατάστασης. Όταν χρησιμοποιείτε την μέθοδο *bootonly*, τα αρχεία μεταφορτώνονται από το δίκτυο κατά απαίτηση.



Σχήμα 7. Εγκατάσταση από το Δίκτυο

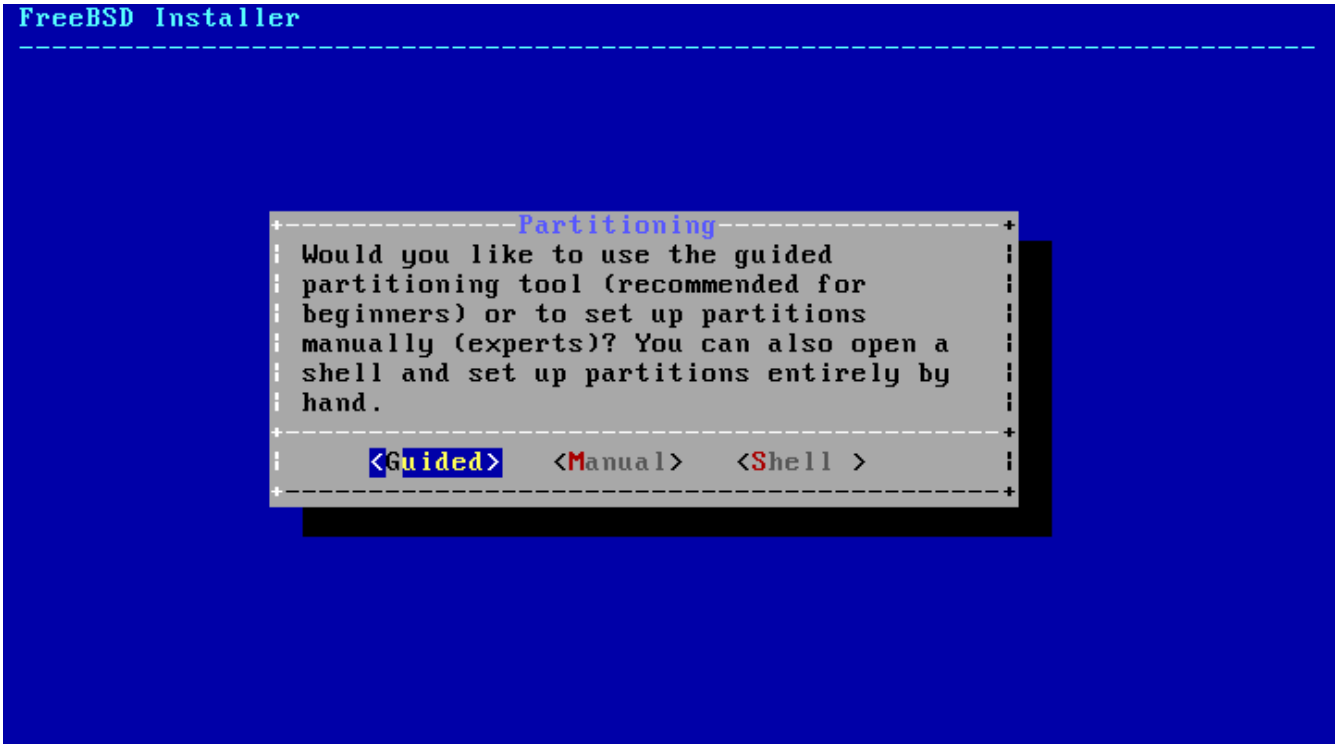
Μετά την ρύθμιση των παραμέτρων δικτύου όπως φαίνεται στο Ρύθμιση Καρτών Δικτύου, γίνεται η επιλογή ενός mirror site. Τα mirror sites διαθέτουν αντίγραφα των αρχείων του FreeBSD. Επιλέξτε ένα mirror site το οποίο βρίσκεται όσο το δυνατόν πιο κοντά στην περιοχή σας. Με τον τρόπο αυτό, η μεταφόρτωση των αρχείων θα είναι ταχύτερη και θα μειωθεί ο χρόνος εγκατάστασης.

Σχήμα 8. Επιλογή Mirror

Η εγκατάσταση θα συνεχιστεί με τον ίδιο τρόπο όπως και αν τα αρχεία ήταν διαθέσιμα τοπικά.

4.7. Εκχώρηση Χώρου στο Δίσκο

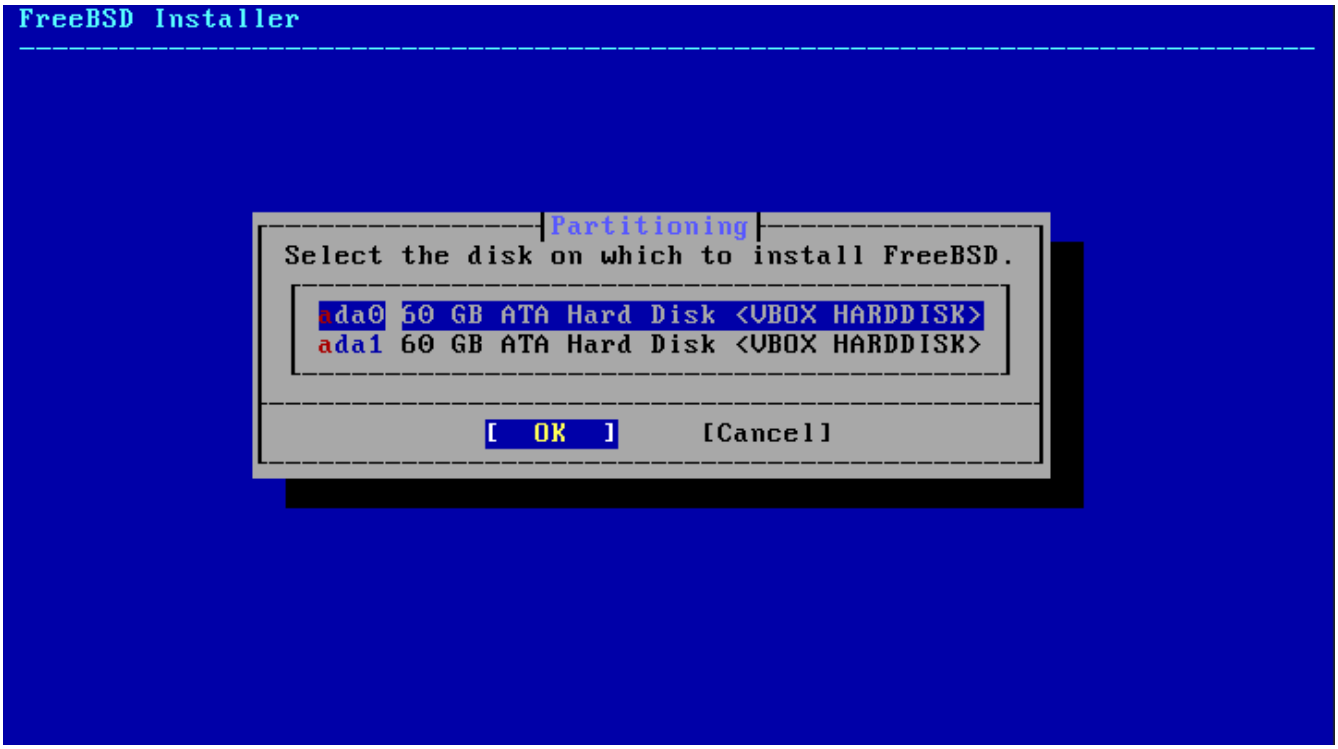
Υπάρχουν τρεις τρόποι να εκχωρήσετε χώρο για το FreeBSD. Με τη μέθοδο *Guided (καθοδηγούμενη)*, οι κατατμήσεις δημιουργούνται αυτόματα, ενώ με τη μέθοδο *Manual (χειροκίνητη)* οι προχωρημένοι χρήστες μπορούν να δημιουργήσουν προσαρμοσμένες κατατμήσεις. Τέλος, υπάρχει η επιλογή να εκκινήσετε ένα κέλυφος και να δημιουργήσετε τις κατατμήσεις με απευθείας χρήση προγραμμάτων της γραμμής εντολών όπως gpart(8), fdisk(8), και bsdlabel(8).



Σχήμα 9. Επιλογή Guided ή Manual Partitioning

4.7.1. Καθοδηγούμενη (Guided) Κατάτμηση

Αν έχετε συνδέσει πολλαπλούς δίσκους, επιλέξτε αυτόν στον οποίο θα εγκαταστήσετε το FreeBSD.

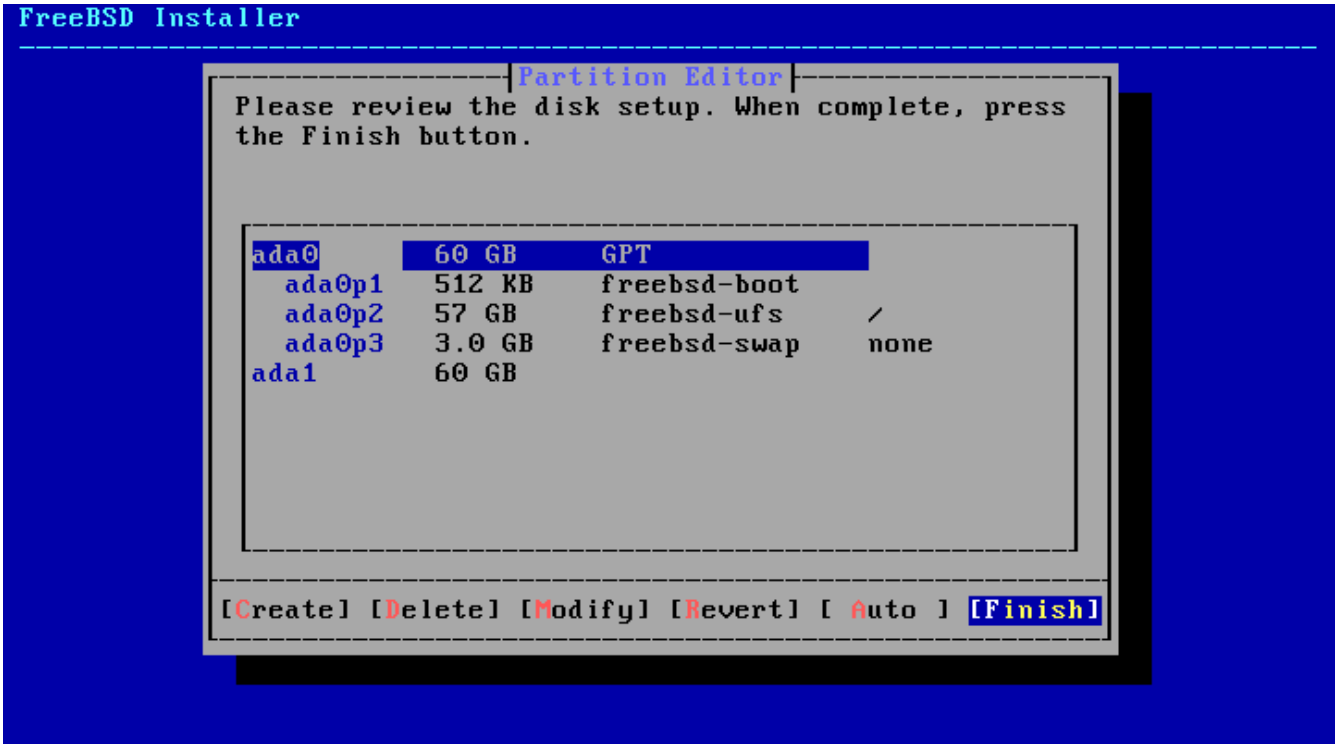


Σχήμα 10. Επιλογή από Πολλαπλούς Δίσκους

Μπορείτε να εκχωρήσετε είτε ολόκληρο το δίσκο, είτε ένα μέρος του στο FreeBSD. Αν επιλέξετε **[Entire Disk]**, θα δημιουργηθούν μια κατάλληλη διάταξη κατατμήσεων ώστε να χρησιμοποιηθεί ολόκληρος ο δίσκος. Αν επιλέξετε **[Partition]**, θα δημιουργηθεί μια διάταξη που θα καταλαμβάνει τον ελεύθερο χώρο του δίσκου.

Σχήμα 11. Επιλογή Ολόκληρου Δίσκου ή Κατάτμησης

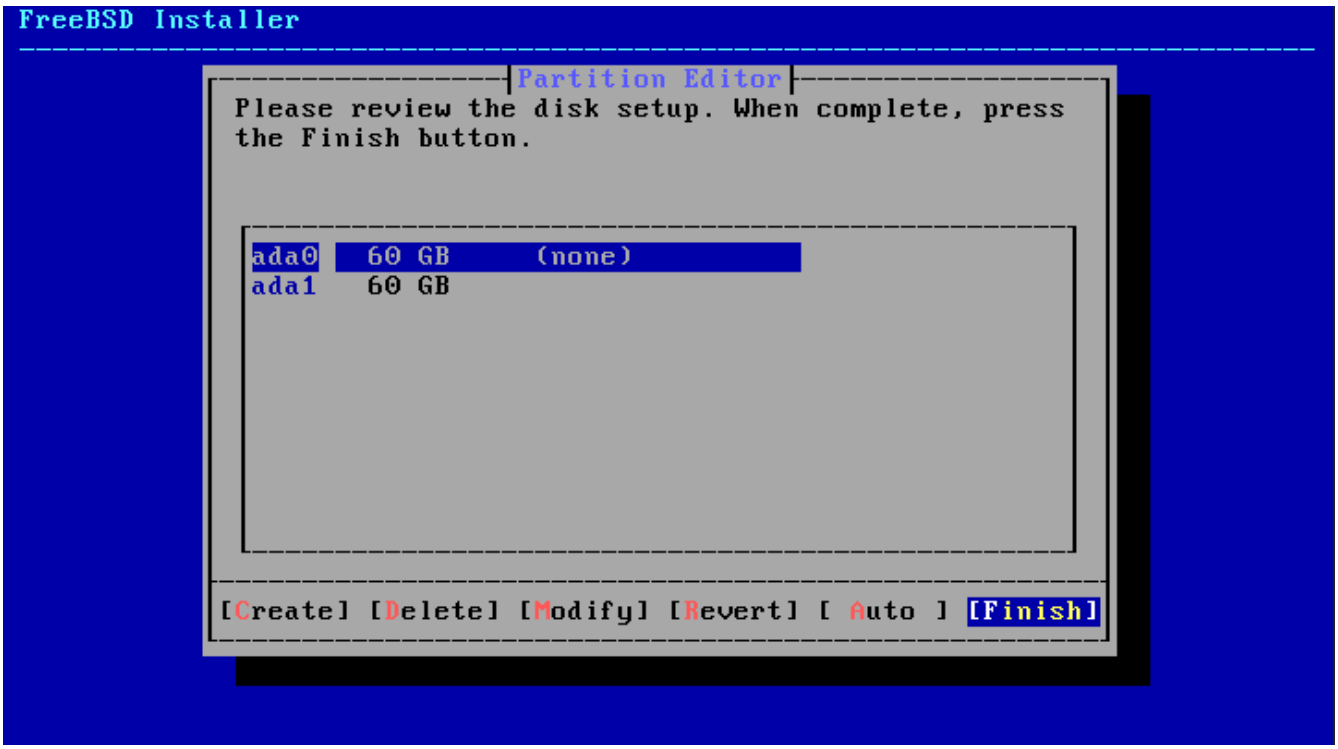
Ελέγξτε προσεκτικά τη διάταξη των κατατμήσεων που δημιουργήθηκε. Αν βρείτε κάποιο λάθος, επιλέξτε **[Revert]** για να επαναφέρετε τις προηγούμενες κατατμήσεις ή **[Auto]** για να δημιουργήσετε τις κατατμήσεις που προτείνονται αυτόματα από το FreeBSD. Μπορείτε να δημιουργήσετε, να τροποποιήσετε και να διαγράψετε κατατμήσεις χειροκίνητα. Όταν οι κατατμήσεις είναι οι σωστές, επιλέξτε **[Finish]** για να συνεχίσετε με την εγκατάσταση.



Σχήμα 12. Επισκόπηση Κατατμήσεων

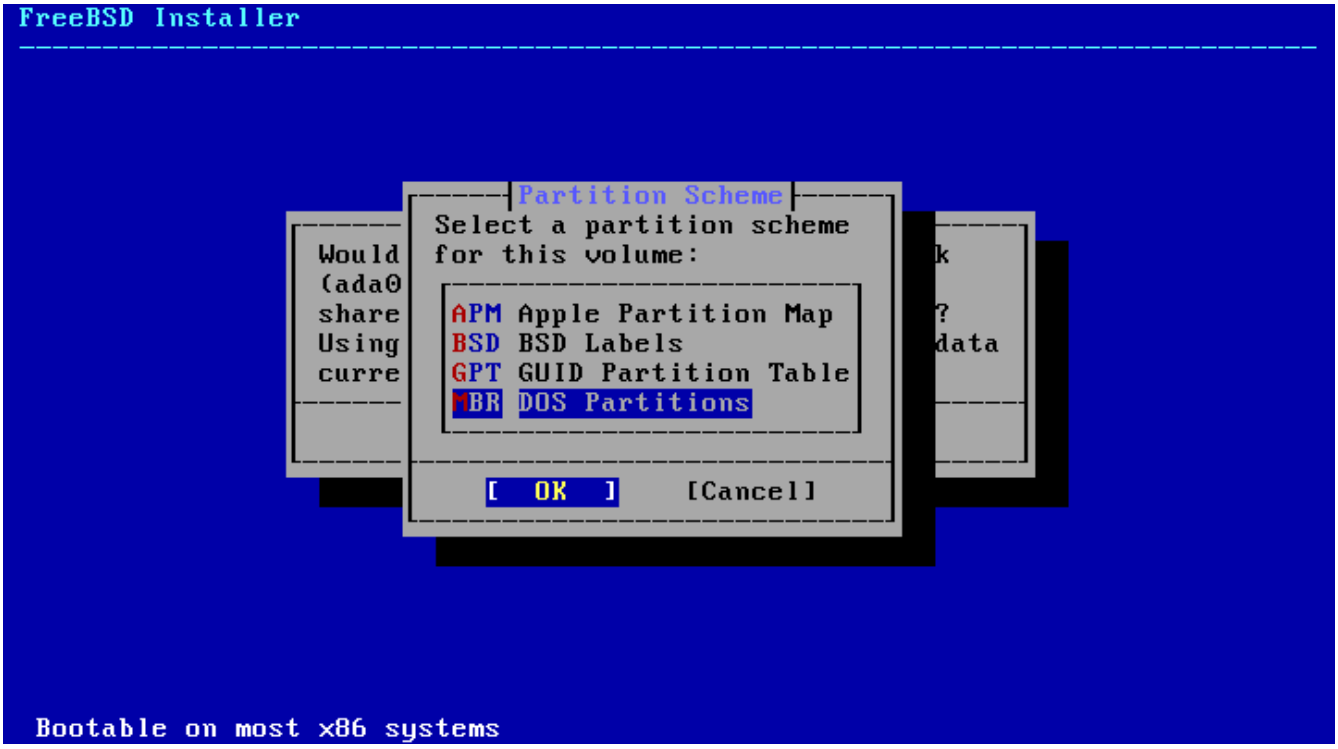
4.7.2. Χειροκίνητη Δημιουργία Κατατμήσεων

Επιλέγοντας χειροκίνητη δημιουργία κατατμήσεων, θα μεταφερθείτε απευθείας στον επεξεργαστή κατατμήσεων.



Σχήμα 13. Χειροκίνητη Δημιουργία Κατατμήσεων

Επιλέγοντας ένα οδηγό (ada0 στο παράδειγμα μας) και το πλήκτρο **[Create]** θα δείτε ένα μενού για την επιλογή του σχήματος κατατμήσεων (*partitioning scheme*).



Σχήμα 14. Χειροκίνητη Δημιουργία Κατατμήσεων

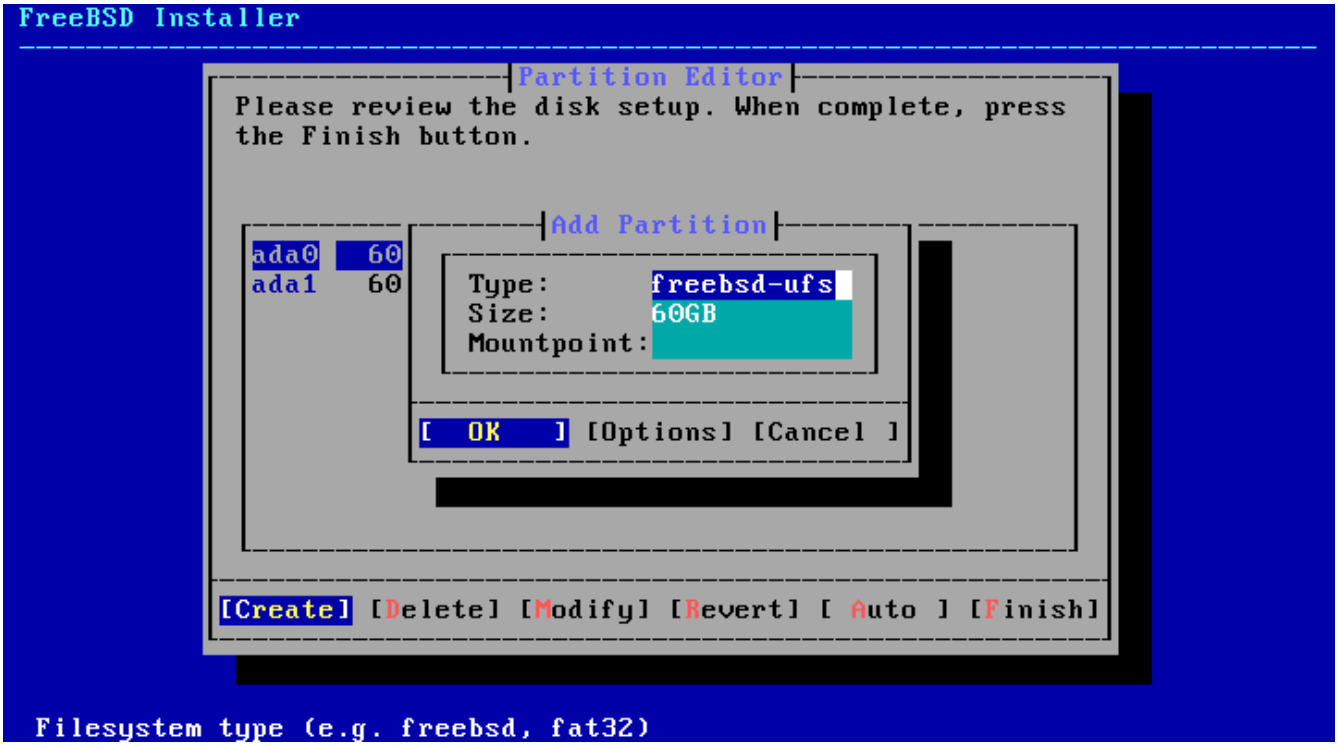
Το σύστημα κατατμήσεων GPT είναι συνήθως το καταλληλότερο για τα περισσότερους PC-

συμβατούς υπολογιστές. Παλαιότερα λειτουργικά συστήματα δεν είναι συμβατά με τη μέθοδο GPT και χρειάζονται κατατμήσεις τύπου MBR. Τα υπόλοιπα είδη κατατμήσεων χρησιμοποιούνται σε παλιά ή μη-συνηθισμένα συστήματα υπολογιστών.

Πίνακας 1. Κατηγορίες Κατατμήσεων

Συντομογραφία	Περιγραφή
APM	Apple Partition Map, χρησιμοποιείται στο PowerPC® Macintosh®.
BSD	Κατατμήσεις BSD χωρίς MBR, ορισμένες φορές καλούνται και "επικίνδυνα αφοσιωμένη κατάσταση". Δείτε το bsdlabel(8).
GPT	Πίνακας Κατατμήσεων GUID.
MBR	Master Boot Record.
PC98	Παραλλαγή του MBR που χρησιμοποιείται σε υπολογιστές NEC PC-98.
VTOC8	Volume Table Of Contents, χρησιμοποιείται στα Sun SPARC64 και UltraSPARC.

Μετά τη δημιουργία του σχήματος κατατμήσεων, αν επιλέξετε ξανά **[Create]** θα δημιουργήσετε νέες κατατμήσεις.



Σχήμα 15. Χειροκίνητη Δημιουργία Κατατμήσεων

Η τυποποιημένη εγκατάσταση FreeBSD με χρήση GPT δημιουργεί τουλάχιστον τρεις κατατμήσεις:

Τυποποιημένες FreeBSD GPT Κατατμήσεις

- `freebsd-boot` - Ο κώδικας εκκίνησης του FreeBSD. Η κατάτμηση αυτή πρέπει να είναι η πρώτη στο δίσκο.

- `freebsd-ufs` - Σύστημα αρχείων FreeBSD UFS.
- `freebsd-swap` - Χώρος swap FreeBSD.

Ένα άλλο αξιοσημείωτο είδος κατάτμησης, είναι το `freebsd-zfs`. Δείτε το Το Σύστημα Αρχείων Z (ZFS). Μπορείτε να δείτε τα υπόλοιπα διαθέσιμα είδη κατατμήσεων GPT στο gpart(8).

Μπορείτε να δημιουργήσετε πολλαπλά συστήματα αρχείων. Κάποιοι χρήστες προτιμούν τη δημιουργία των παραδοσιακών κατατμήσεων με χωριστά συστήματα αρχείων για τα /, /var, και /usr. Δείτε το Δημιουργία Παραδοσιακών Κατατμήσεων στο Σύστημα Αρχείων για ένα παράδειγμα.

Μπορείτε να εισάγετε το μέγεθος με τη βοήθεια κοινών συντομεύσεων: *K* για kilobytes, *M* για megabytes, ή *G* για gigabytes.

Η καλύτερη απόδοση επιτυγχάνεται με ευθυγράμμιση των τομέων του δίσκου (sector alignment). Η σωστή ευθυγράμμιση επιτυγχάνεται με τη δημιουργία κατατμήσεων με μεγέθη πολλαπλάσια των 4K bytes σε οδηγούς που χρησιμοποιούν τομείς των 512 bytes ή 4K-byte. Σε γενικές γραμμές, η χρήση κατατμήσεων με μεγέθη που είναι άρτια πολλαπλάσια του 1M ή 1G είναι ο ευκολότερος τρόπος να επιβεβαιώσουμε ότι κάθε κατάτμηση ξεκινά σε ζυγό πολλαπλάσιο των 4K. Μια εξαίρεση: την παρούσα στιγμή η κατάτμηση *freebsd-boot* δεν μπορεί να είναι μεγαλύτερη των 512K λόγων περιορισμών του κώδικα εκκίνησης.

Σε κάθε κατάτμηση που περιέχει σύστημα αρχείων, χρειάζεται ένα σημείο προσάρτησης. Αν χρησιμοποιηθεί μόνο μια κατάτμηση UFS, το σημείο προσάρτησης θα είναι η /.

θα σας ζητηθεί επίσης μια ετικέτα (*label*). Η ετικέτα είναι ένα όνομα το οποίο δίνεται σε μια κατάτμηση. Το όνομα ενός δίσκου ή οι αριθμοί που περιγράφουν τις κατατμήσεις μπορεί να αλλάξουν αν ο δίσκος συνδεθεί σε άλλη θύρα ή ελεγκτή, αλλά η ετικέτα του παραμένει σταθερή. Με χρήση της ετικέτας σε αρχεία όπως το /etc/fstab το σύστημα γίνεται πιο ανεκτικό σε αλλαγές του υλικού. Οι ετικέτες GPT εμφανίζονται στον κατάλογο /dev/gpt/ όταν γίνεται η προσάρτηση της συσκευής. Σε άλλα είδη κατατμήσεων υπάρχουν διαφορετικές δυνατότητες όσο αφορά τις ετικέτες, οι οποίες εμφανίζονται σε διαφορετικούς υποκαταλόγους στο /dev/.

Χρησιμοποιήστε μοναδικές ετικέτες σε κάθε σύστημα αρχείων για να αποφύγετε συγκρούσεις που μπορεί να προκληθούν από όμοια ονόματα. Σε κάθε ετικέτα μπορείτε να συμπεριλάβετε μερικά γράμματα από το όνομα του υπολογιστή ή τη θέση του, ή ακόμα και τη χρήση του. Θα μπορούσατε για παράδειγμα να ονομάσετε τον κεντρικό κατάλογο `labroot` ή `rootfs-lab` σε ένα υπολογιστή που ανήκει σε ένα εργαστήριο.

Παράδειγμα 3. Δημιουργία Παραδοσιακών Κατατμήσεων στο Σύστημα Αρχείων

Αν επιθυμείτε να χρησιμοποιήσετε το παραδοσιακό σύστημα κατατμήσεων του FreeBSD όπου τα συστήματα αρχείων /, /var, /tmp και /usr βρίσκονται σε χωριστές κατατμήσεις, δημιουργήστε ένα πίνακα κατατμήσεων GPT και ορίστε τις κατατμήσεις με τον τρόπο που φαίνεται παρακάτω. Τα μεγέθη που φαίνονται είναι τυπικά για ένα σκληρό δίσκο χωρητικότητας 20G. Αν διαθέτετε περισσότερο χώρο, ίσως είναι χρήσιμο να μεγαλώσετε την κατάτμηση swap ή /var. Στο παράδειγμα μας, οι ετικέτες που χρησιμοποιούνται ξεκινούν με `ex` (από τη λέξη "example")

αλλά καλό θα είναι να χρησιμοποιήσετε δικές σας μονάδικες ετικέτες όπως αναφέραμε παραπάνω.

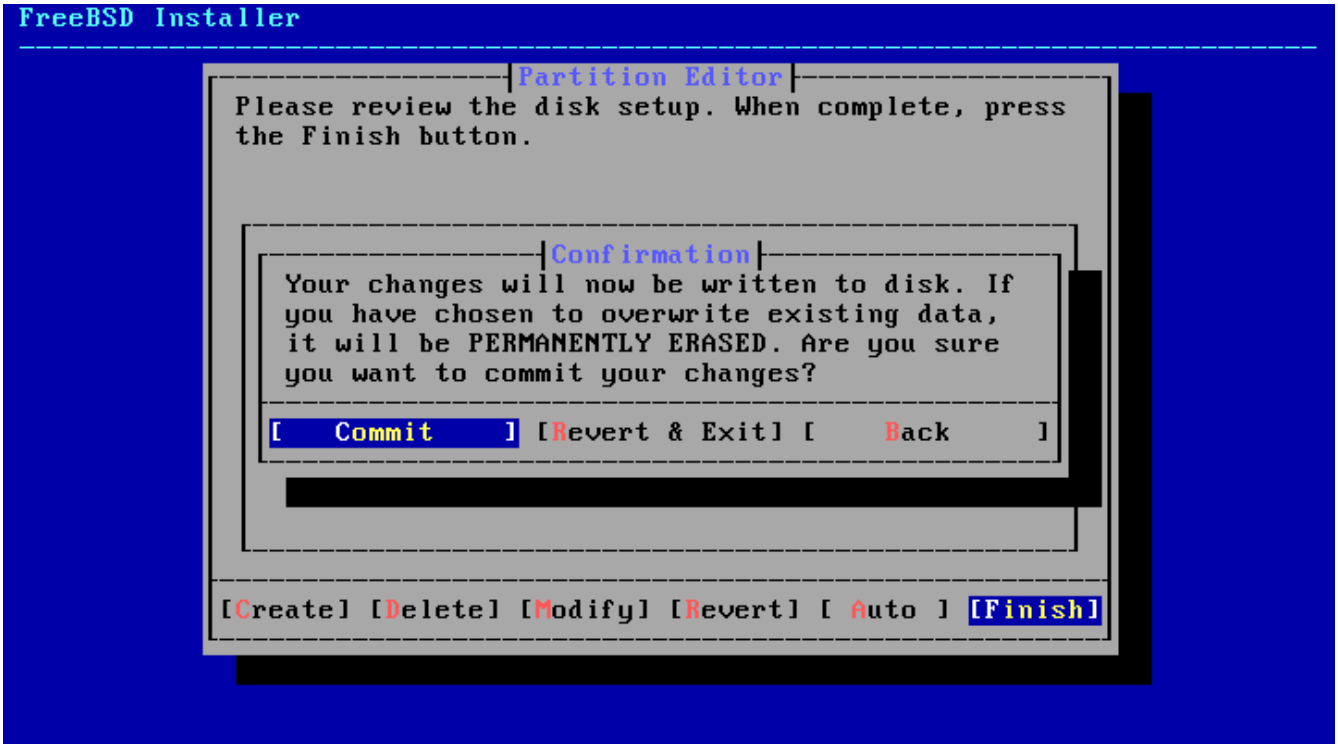
Από προεπιλογή, το gptboot του FreeBSD αναμένει την πρώτη UFS κατάτμηση ως /.

Τύπος Κατάτμησης	Μέγεθος	Σημείο Προσάρτησης	Ετικέτα
freebsd-boot	512K		
freebsd-ufs	2G	/	exrootfs
freebsd-swap	4G		exswap
freebsd-ufs	2G	/var	exvarfs
freebsd-ufs	1G	/tmp	extmpfs
freebsd-ufs	αποδεχθείτε την προεπιλογή (υπόλοιπος χώρος του δίσκου)	/usr	exusrfs

Μετά τη δημιουργία των προσαρμοσμένων κατατμήσεων, επιλέξτε **[Finish]** για να συνεχίσετε με την εγκατάσταση.

4.8. Επιβεβαίωση της Εγκατάστασης

Σε αυτό το σημείο έχετε την τελευταία ευκαιρία να εγκαταλείψετε την εγκατάσταση χωρίς να γίνουν αλλαγές στο σκληρό δίσκο σας.



Σχήμα 16. Τελική Επιβεβαίωση

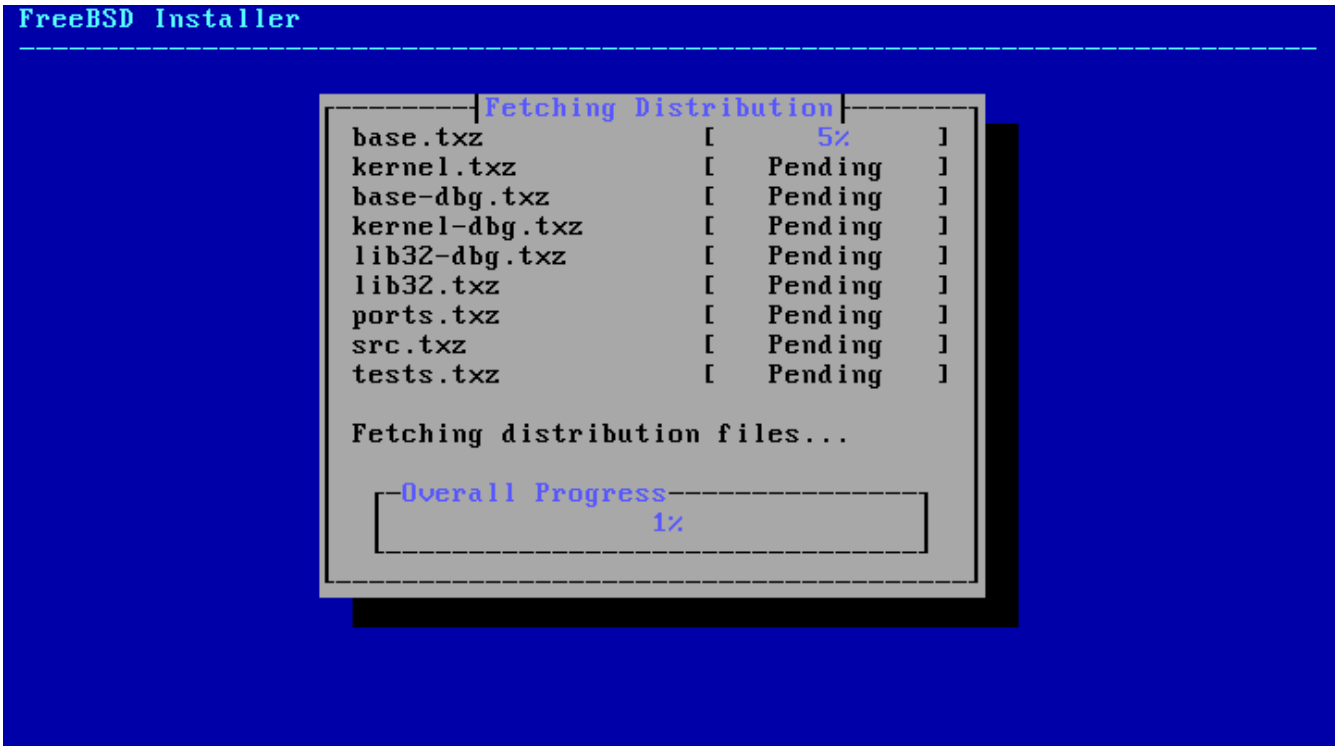
Επιλέξτε **[Commit]** και πιέστε `Enter` για να συνεχίσετε. Αν χρειάζεται να κάνετε αλλαγές, επιλέξτε **[Back]** για να επιστρέψετε στον επεξεργαστή κατατμήσεων. Με το πλήκτρο **[Revert & Exit]**

μπορείτε να εγκαταλείψετε το πρόγραμμα εγκατάστασης χωρίς να γίνουν αλλαγές στο σκληρό σας δίσκο.

Ο χρόνος εγκατάστασης ποικίλει ανάλογα με τις διανομές και τα στοιχεία εγκατάστασης που έχετε επιλέξει, το μέσο εγκατάστασης και την ταχύτητα του υπολογιστή. Θα δείτε μια σειρά από μηνύματα σχετικά με την πρόοδο της διαδικασίας.

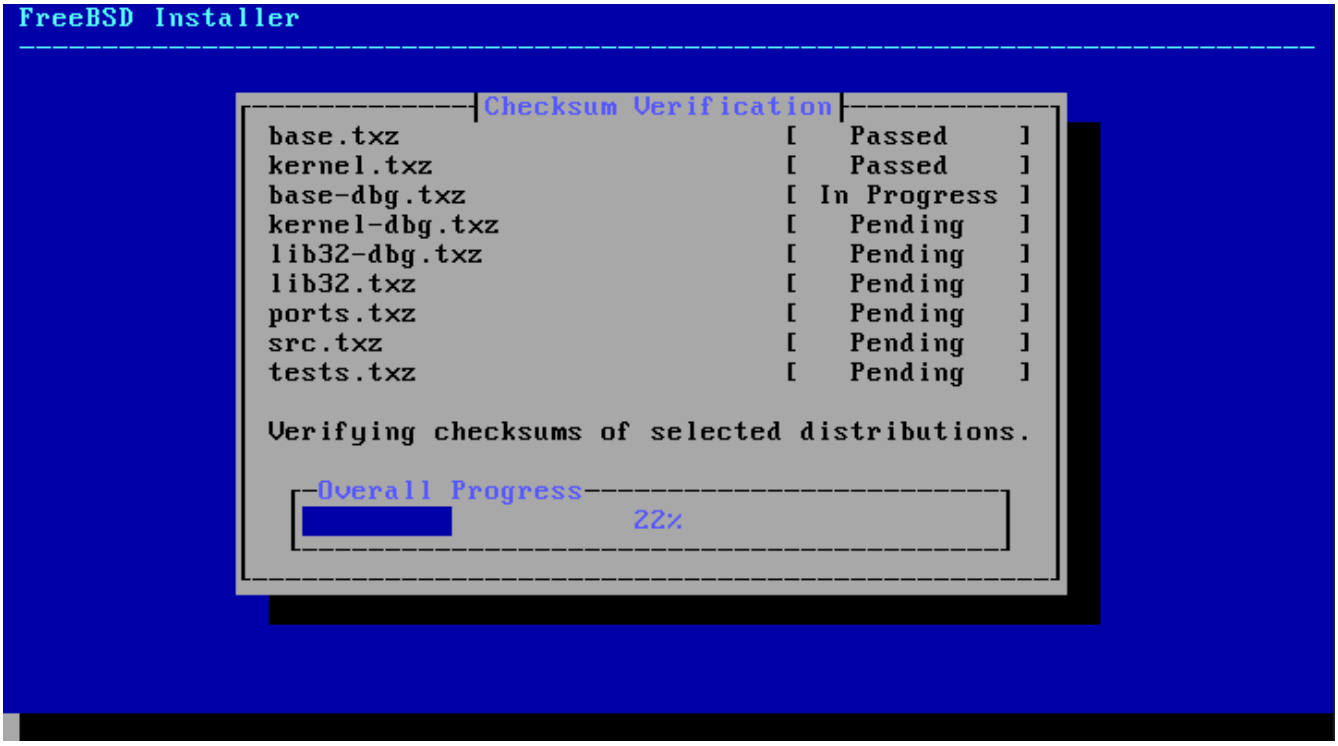
Αρχικά, το πρόγραμμα εγκατάστασης θα γράψει τις κατατμήσεις στο δίσκο και θα εκτελέσει κατάλληλες εντολές `newfs` για να δημιουργήσει τα ανάλογα συστήματα αρχείων.

Αν κάνετε εγκατάσταση μέσω δικτύου, το bsdinstall θα προχωρήσει μεταφορτώνοντας τα απαραίτητα αρχεία.



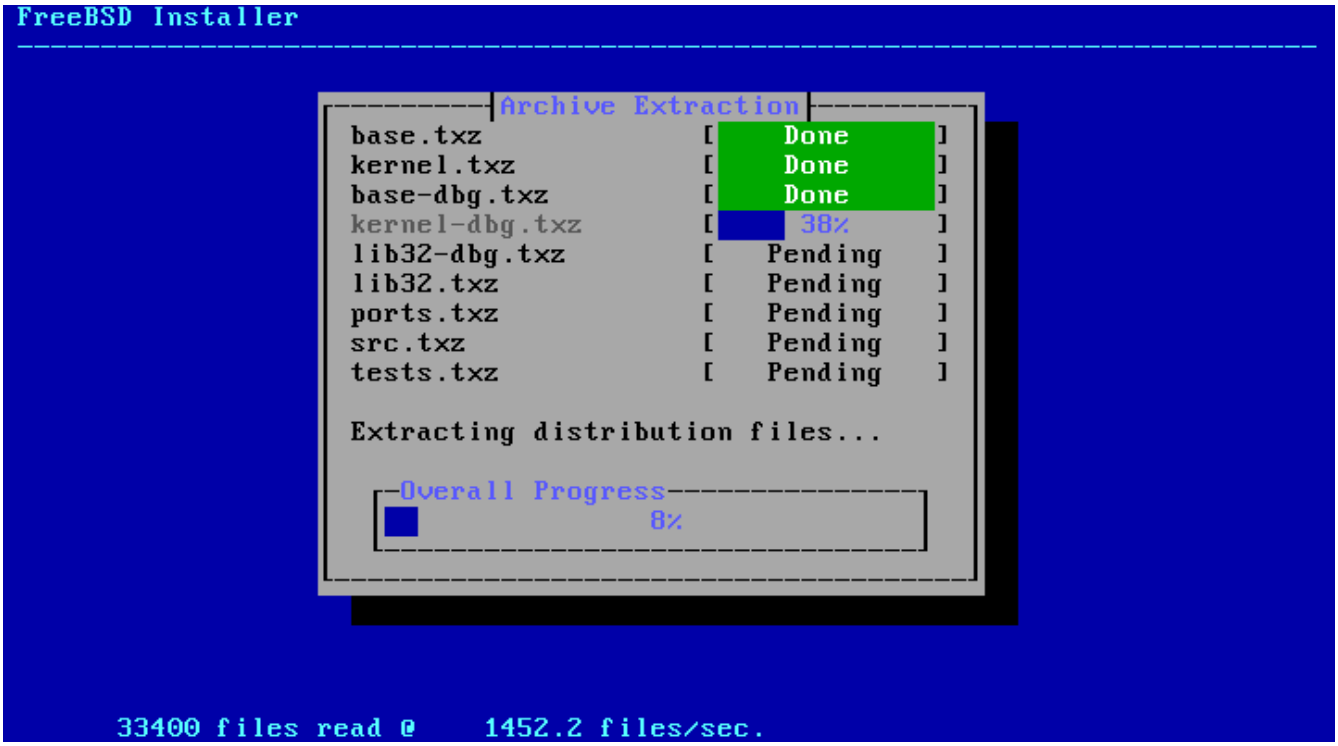
Σχήμα 17. Μεταφόρτωση Αρχείων Εγκατάστασης

Στη συνέχεια, θα γίνει έλεγχος ακεραιότητας των αρχείων εγκατάστασης για να επιβεβαιωθεί ότι δεν έχουν αλλοιωθεί κατά τη μεταφόρτωση ή κατά την ανάγνωση από το μέσο εγκατάστασης.



Σχήμα 18. Επαλήθευση Αρχείων Εγκατάστασης

Στο τελευταίο βήμα, τα επιβεβαιωμένα αρχεία εγκατάστασης θα εξαχθούν και θα γραφούν στο σκληρό δίσκο.



Σχήμα 19. Εξαγωγή Αρχείων Εγκατάστασης

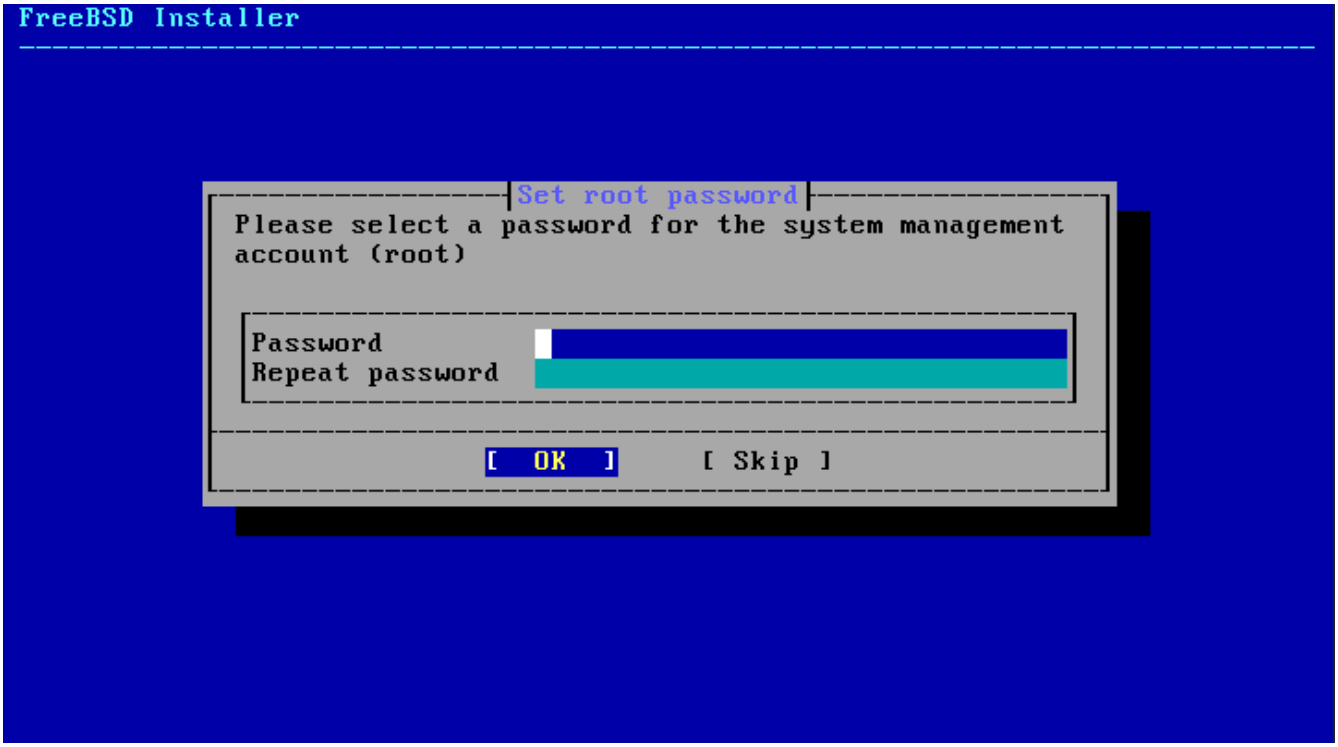
Με το τέλος της εξαγωγής όλων των αρχείων εγκατάστασης, το bsdinstall θα εισέλθει στη διαδικασία ρυθμίσεων μετά την εγκατάσταση (δείτε Μετά την Εγκατάσταση).

4.9. Μετά την Εγκατάσταση

Μετά από μια επιτυχημένη εγκατάσταση του FreeBSD, ακολουθεί μια σειρά ρυθμίσεων. Μπορείτε να επαναλάβετε οποιαδήποτε ρύθμιση αν εισέλθετε στην αντίστοιχη επιλογή στο τελικό μενού πριν επανεκκινήσετε στο νέο-εγκατεστημένο σας FreeBSD σύστημα.

4.9.1. Ρύθμιση του Κωδικού του `root`

Θα πρέπει να ορίσετε ένα κωδικό πρόσβασης για το χρήστη `root`. Παρατηρήστε ότι δεν φαίνονται τα γράμματα που πληκτρολογείτε καθώς εισάγετε τον κωδικό. Μετά την εισαγωγή του κωδικού, θα πρέπει να τον εισάγετε ακόμα μια φορά. Με τον τρόπο αυτό εξασφαλίζεται ότι δεν έχει γίνει κάποιο λάθος κατά την πληκτρολόγηση.



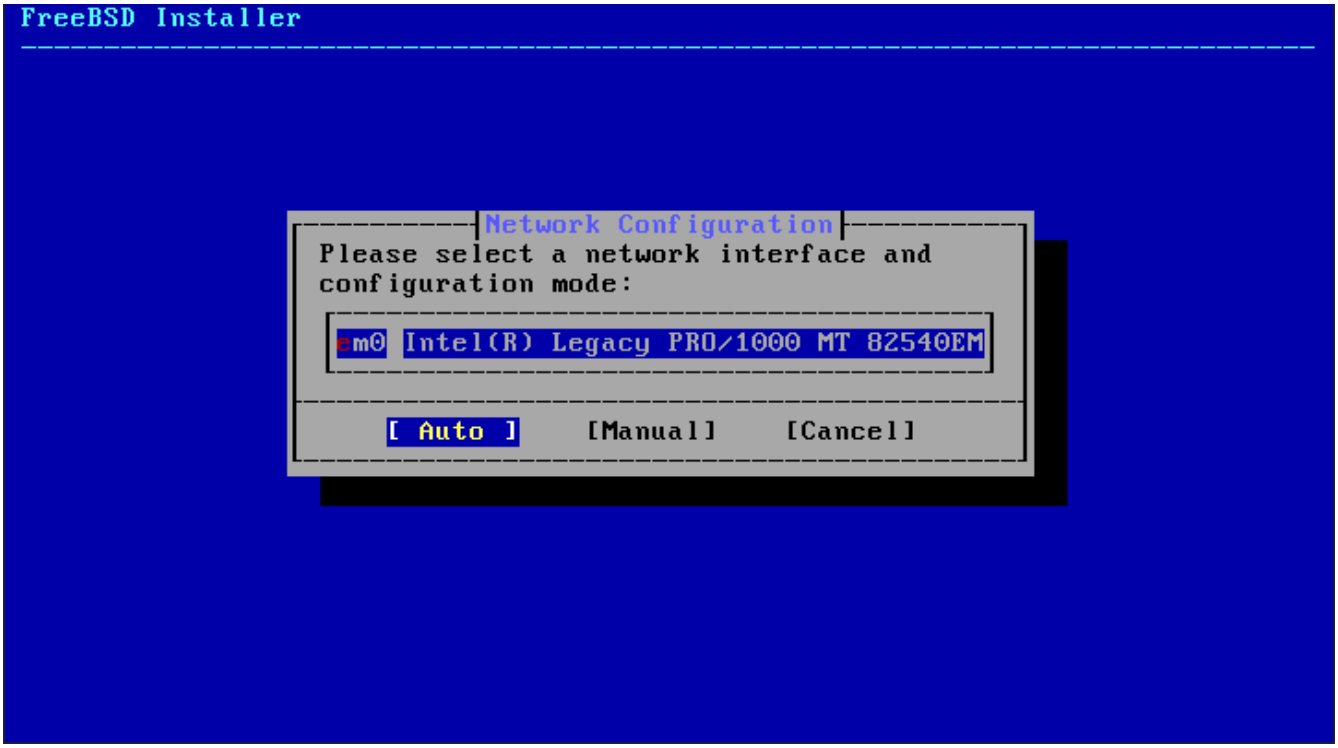
Σχήμα 20. Ρύθμιση του Κωδικού του `root`

Η εγκατάσταση συνεχίζεται μετά την επιτυχή εισαγωγή του κωδικού.

4.9.2. Ρύθμιση Καρτών Δικτύου

Η ρύθμιση του δικτύου παραλείπεται αν έχει ήδη πραγματοποιηθεί στα πλαίσια μιας εγκατάστασης *bootonly*.

Θα δείτε μια λίστα με όλες τις διεπαφές δικτύου που ανιχνεύθηκαν στον υπολογιστή σας. Επιλέξτε αυτή που επιθυμείτε να ρυθμίσετε.



Σχήμα 21. Επιλογή μιας Διεπαφής Δικτύου

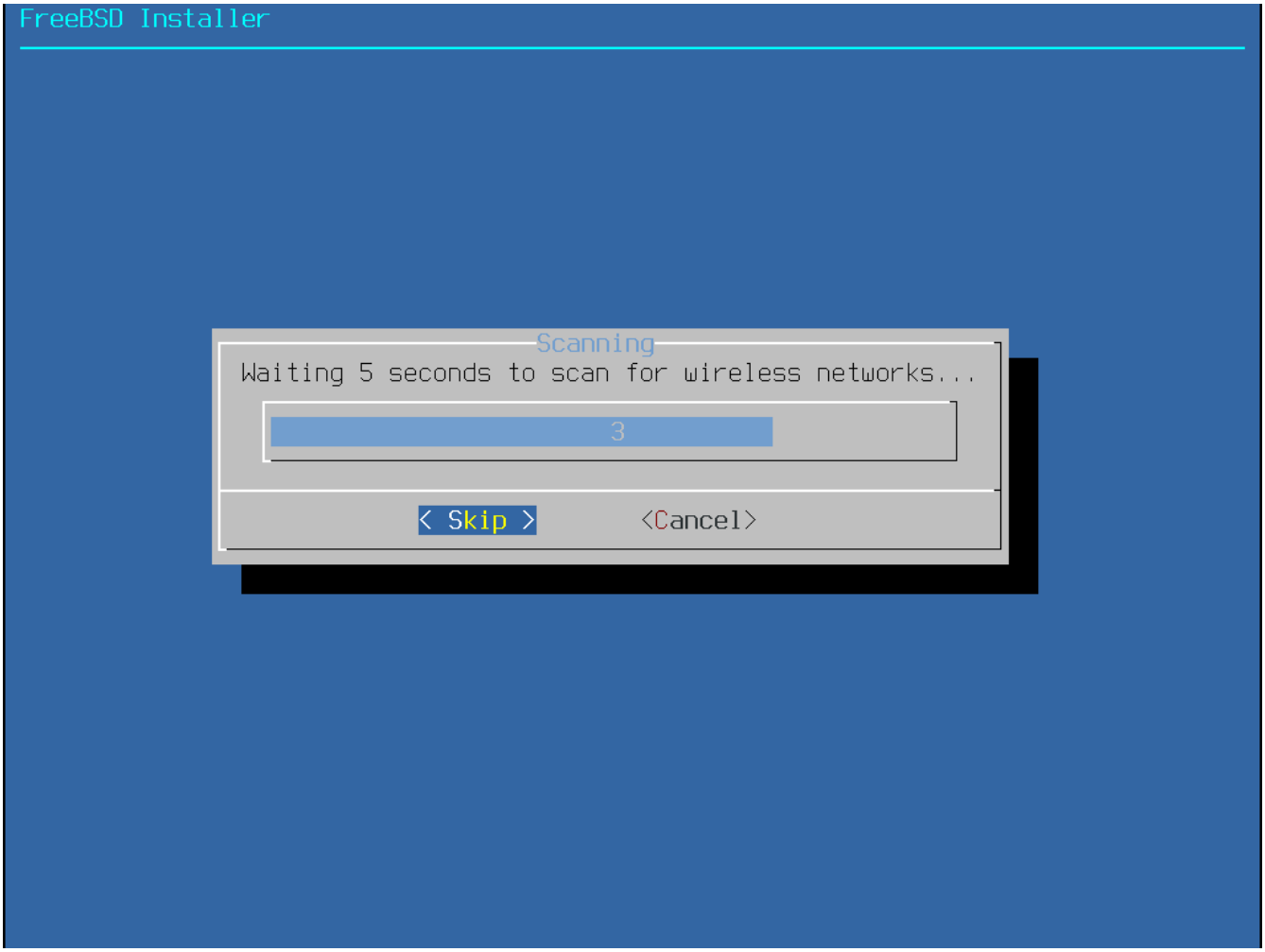
4.9.2.1. Ρύθμιση Ασύρματης Κάρτας Δικτύου

Αν επιλέξετε να ρυθμίσετε μια ασύρματη διεπαφή δικτύου, θα πρέπει να ρυθμίσετε τις παραμέτρους αναγνώρισης και ασφάλειας για να συνδεθείτε στο δίκτυο.

Τα ασύρματα δίκτυα αναγνωρίζονται από το Αναγνωριστικό Υπηρεσίας ή Service Set Identifier (SSID). Το SSID είναι ένα σύντομο μοναδικό όνομα που αποδίδεται σε κάθε ασύρματο δίκτυο.

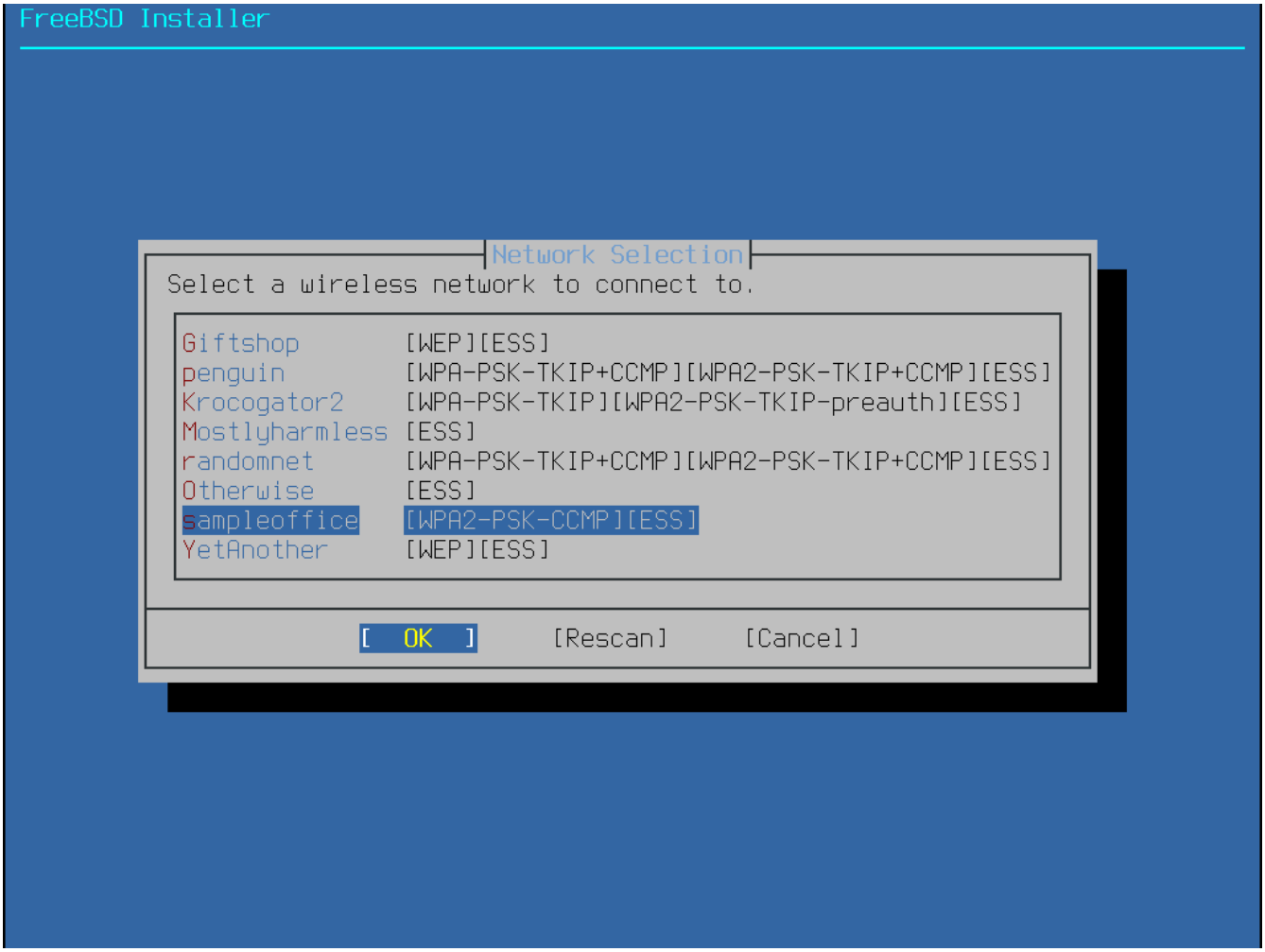
Τα περισσότερα ασύρματα δίκτυα κρυπτογραφούν τα δεδομένα που μεταδίδονται για να προστατεύσουν τις πληροφορίες από μη εξουσιοδοτημένη χρήση. Συνίσταται να χρησιμοποιήσετε κρυπτογράφηση WPA2. Παλαιότερες μέθοδοι κρυπτογράφησης όπως το WEP προσφέρουν ελάχιστη ασφάλεια.

Το πρώτο βήμα για να συνδεθείτε σε ένα ασύρματο δίκτυο είναι να σαρώσετε για Σημεία Ασύρματης Πρόσβασης (Access Points).



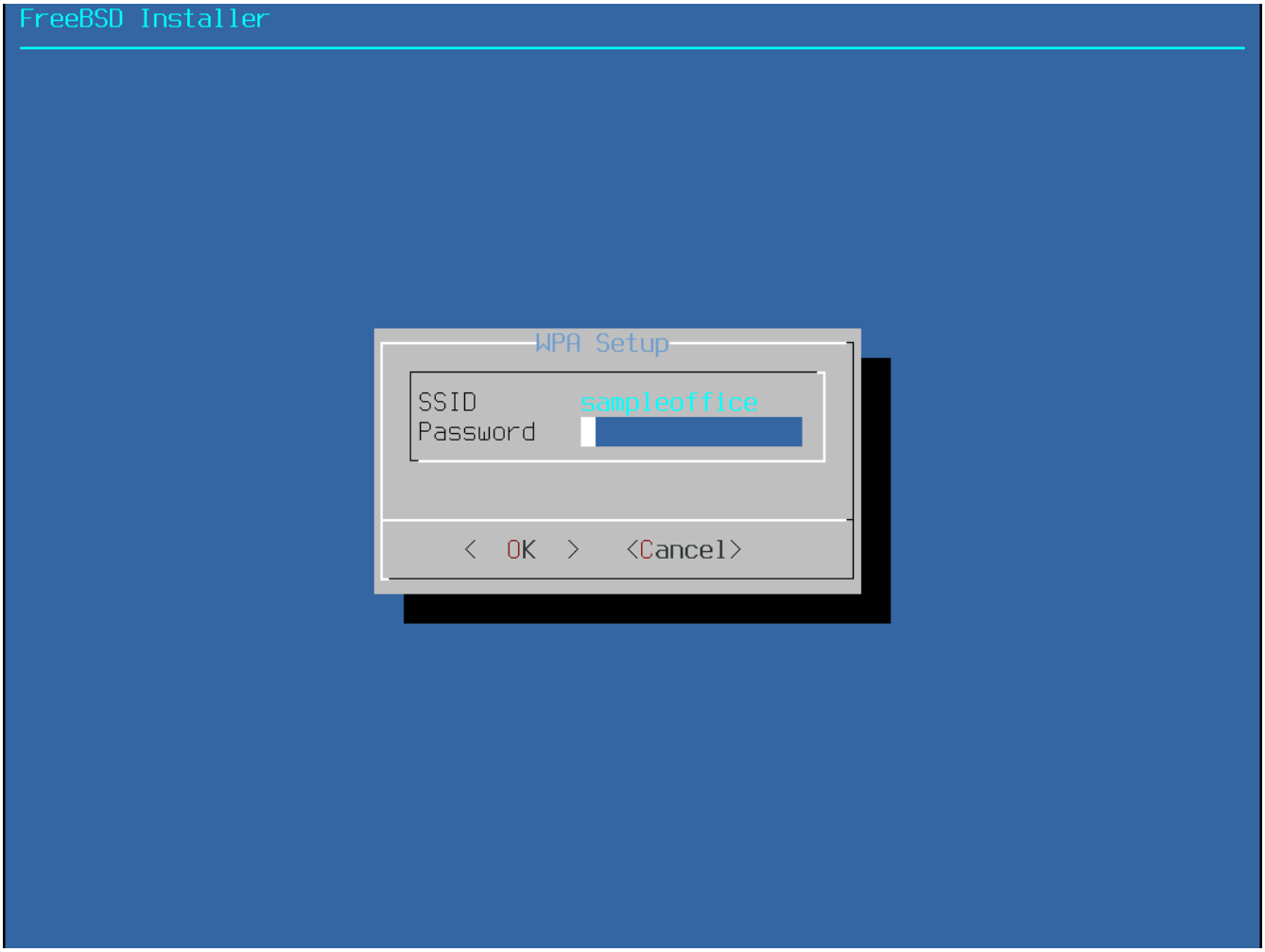
Σχήμα 22. Σάρωση για Access Points

Τα SSIDs που θα βρείτε κατά τη διάρκεια της σάρωσης συνοδεύονται από τα είδη κρυπτογράφησης που διατίθενται για κάθε δίκτυο. Αν δεν βλέπετε το SSID που επιθυμείτε στη λίστα, επιλέξτε **[Rescan]** για να εκτελέσετε τη σάρωση ξανά. Αν εξακολουθείτε να μη βλέπετε το επιθυμητό δίκτυο, ελέγξτε την κεραία για τυχόν προβλήματα ή μετακινήστε τον υπολογιστή πιο κοντά στο σημείο πρόσβασης. Να εκτελείτε νέα σάρωση μετά από κάθε αλλαγή.



Σχήμα 23. Επιλογή Ασύρματου Δικτύου

Μετά την επιλογή του ασύρματου δικτύου, θα πρέπει να εισάγετε τις πληροφορίες που σχετίζονται με την κρυπτογράφηση. Σε δίκτυα WPA2 χρειάζεται να δώσετε μόνο ένα κωδικό πρόσβασης (γνωστό ως Pre-Shared Key ή PSK). Για λόγους ασφαλείας, οι χαρακτήρες που πληκτρολογείτε στο πεδίο εμφανίζονται ως αστερίσκοι.

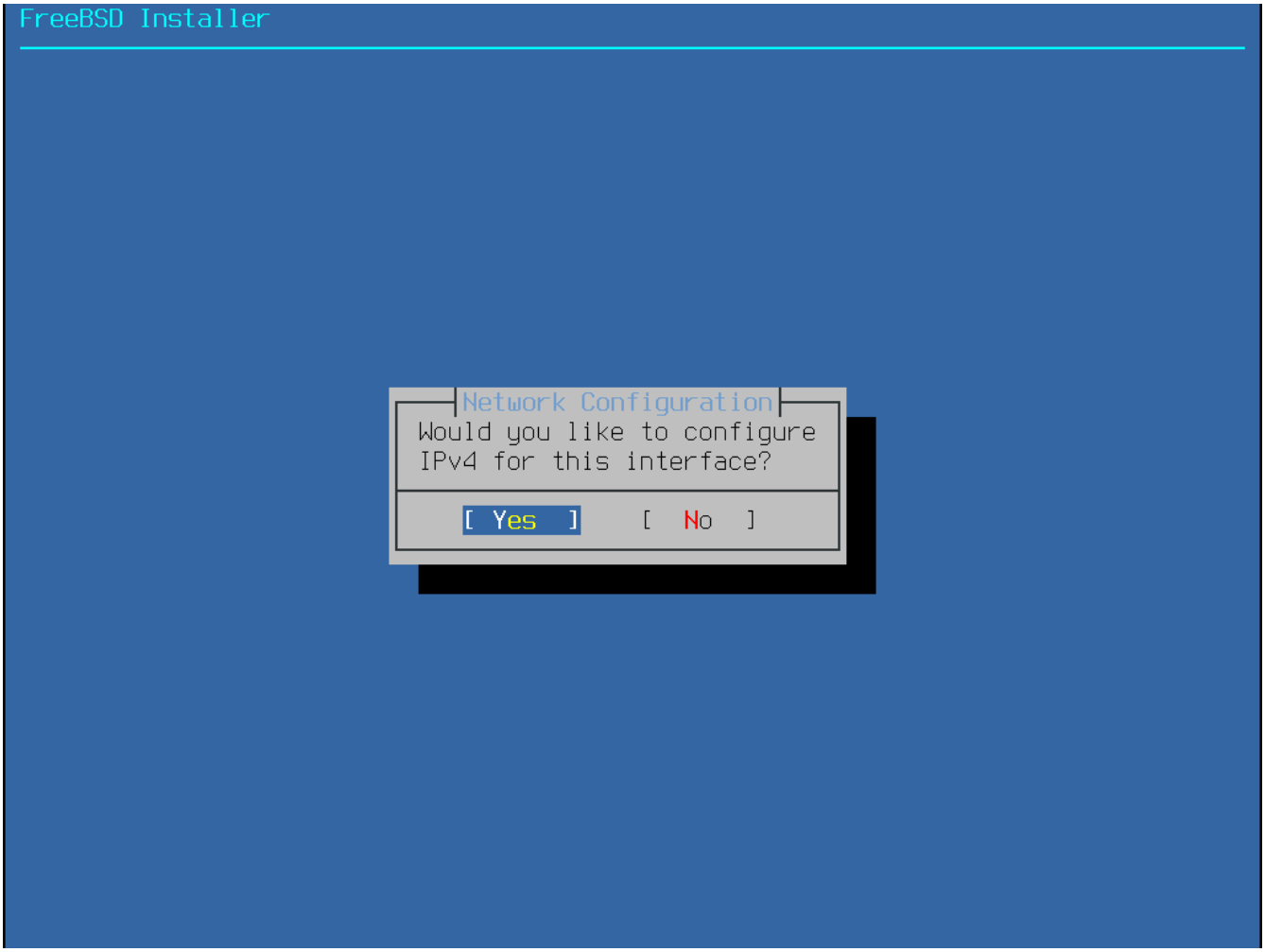


Σχήμα 24. Ρύθμιση WPA2

Μετά την επιλογή του ασύρματου δικτύου και την εισαγωγή των πληροφοριών σύνδεσης, η εγκατάσταση συνεχίζεται με τη ρύθμιση των υπόλοιπων παραμέτρων του δικτύου.

4.9.2.2. Ρύθμιση Δικτύου IPv4

Επιλέξτε αν θα χρησιμοποιηθεί δικτύωση IPv4. Πρόκειται για το πιο συνηθισμένο είδος σύνδεσης.



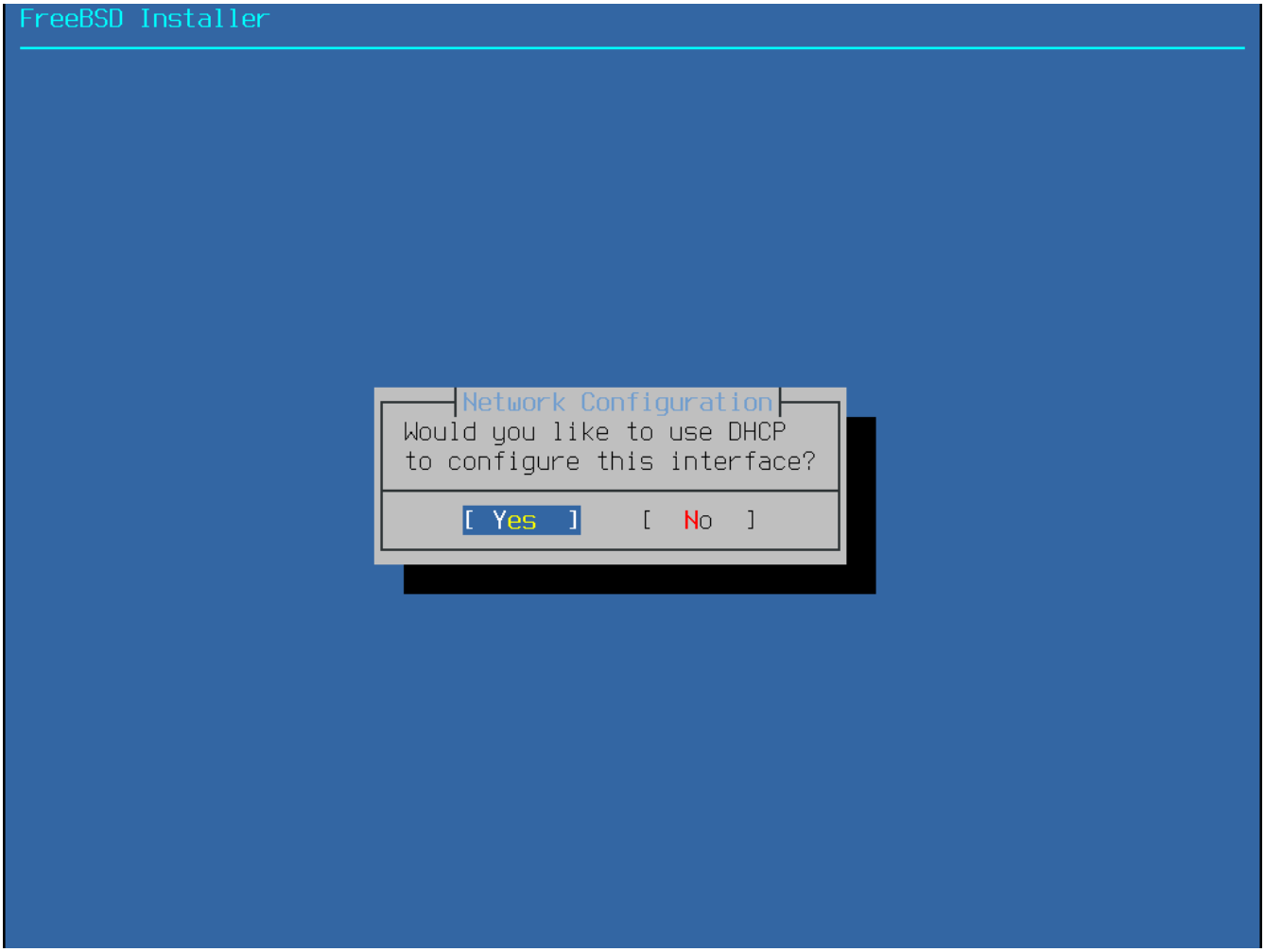
Σχήμα 25. Επιλογή Δικτύωσης IPv4

Υπάρχουν δύο μέθοδοι ρύθμισης του IPv4. Μέσω του *DHCP* η ρύθμιση της διεπαφής γίνεται αυτόματα. Αυτή είναι και η συνιστώμενη μέθοδος. Η ρύθμιση *Static* απαιτεί χειροκίνητη εισαγωγή πληροφοριών δικτύου.

Μη βάλετε τυχαίες ρυθμίσεις δικτύου, καθώς δεν θα λειτουργήσουν. Θα πρέπει να λάβετε τις πληροφορίες που αναφέρονται στο Συλλέξτε Πληροφορίες για το Δίκτυο από τον διαχειριστή ή τον παροχέα του δικτύου σας.

4.9.2.2.1. Ρύθμιση Δικτύου IPv4 μέσω DHCP

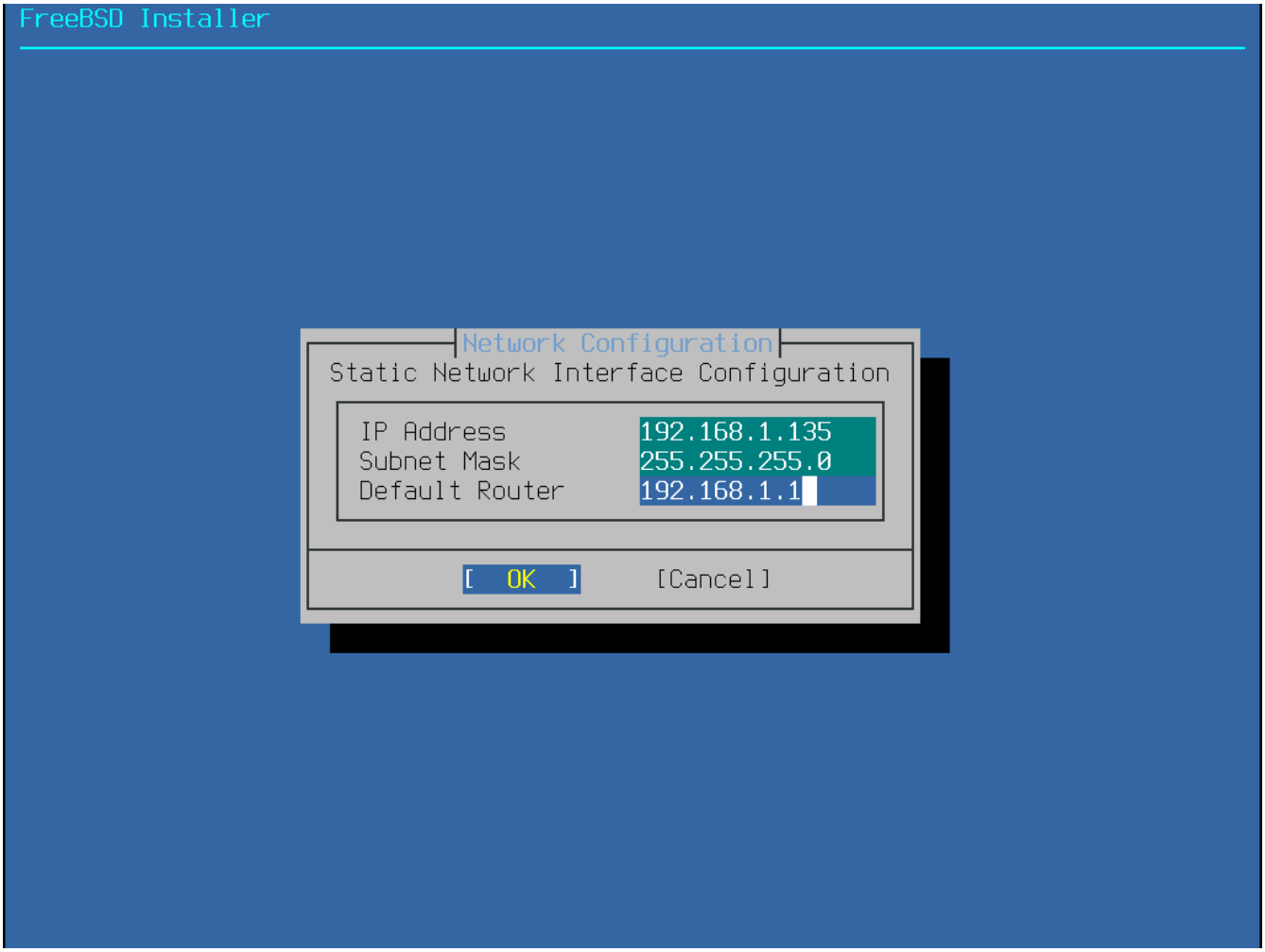
Αν διαθέτετε εξυπηρετητή DHCP, επιλέξτε **[Yes]** για να ρυθμίσετε αυτόματα την διεπαφή δικτύου.



Σχήμα 26. Επιλέξτε Ρύθμιση IPv4 μέσω DHCP

4.9.2.2.2. Στατική Ρύθμιση Δικτύου IPv4

Η στατική ρύθμιση της διεπαφής δικτύου, απαιτεί να εισάγετε κάποιες πληροφορίες σχετικά με το IPv4.

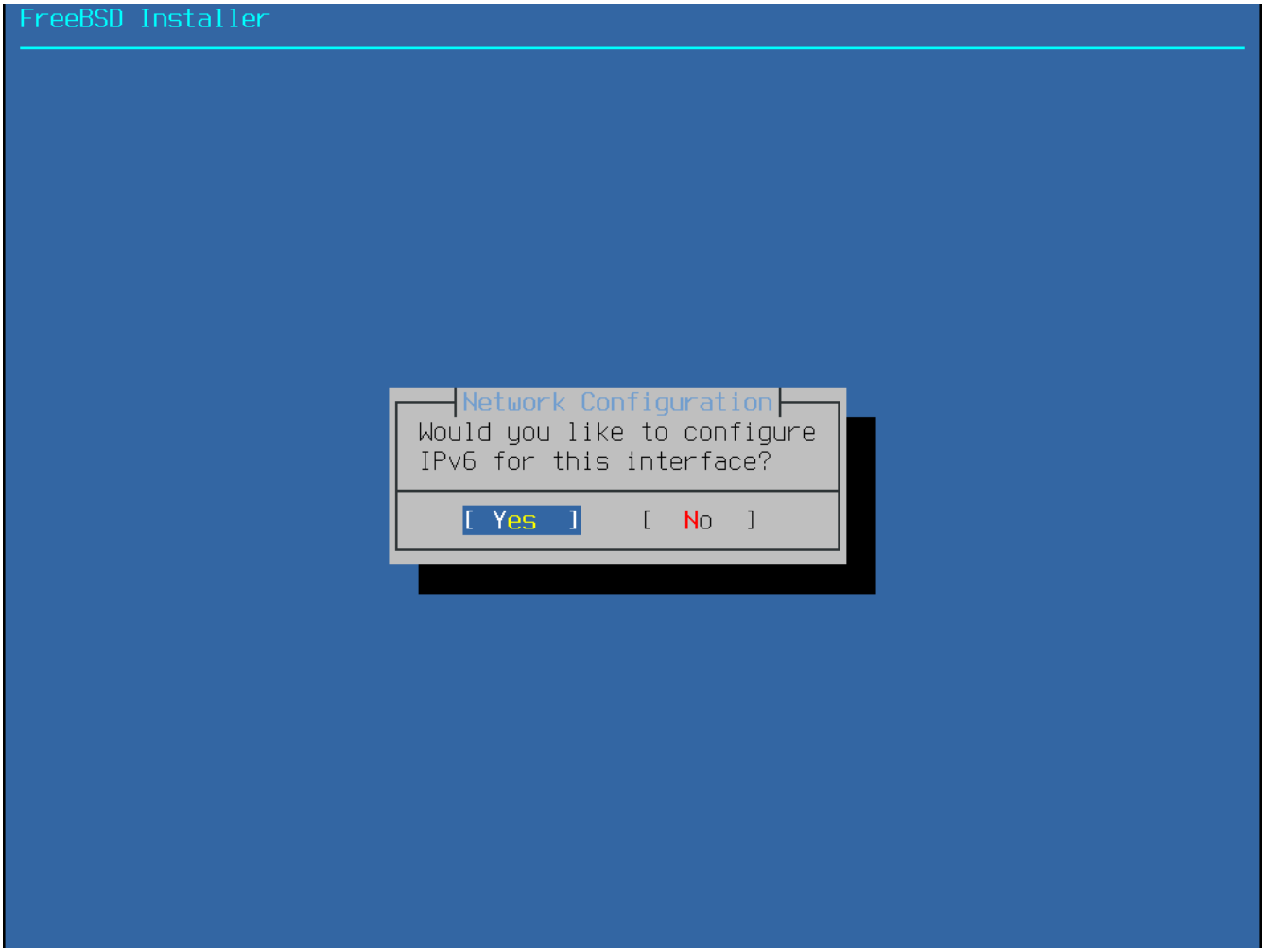


Σχήμα 27. Στατική Ρύθμιση IPv4

- `IP Address` - Η διεύθυνση IP που θα εισάγετε χειροκίνητα σε αυτό τον υπολογιστή. Η διεύθυνση αυτή πρέπει να είναι μοναδική και να μην χρησιμοποιείται από οποιοδήποτε άλλο μηχάνημα στο τοπικό σας δίκτυο.
- `Subnet Mask` - Η μάσκα υποδικτύου που χρησιμοποιεί το τοπικό σας δίκτυο. Τυπικά αυτή είναι `255.255.255.0`.
- `Default Router` - Η διεύθυνση IP του προεπιλεγμένου δρομολογητή του δικτύου σας. Συνήθως είναι η διεύθυνση του δρομολογητή ή άλλου δικτυακού εξοπλισμού που συνδέει το τοπικό σας δίκτυο με το Internet. Θα τη δείτε επίσης να αναφέρετε ως *default gateway (προεπιλεγμένη πύλη)*.

4.9.2.3. Ρύθμιση Δικτύου IPv6

Το IPv6 είναι μια νέα μέθοδος ρύθμισης δικτύου. Αν το δίκτυο σας διαθέτει IPv6 και επιθυμείτε να το ρυθμίσετε, πιέστε **[Yes]** για να το επιλέξετε.

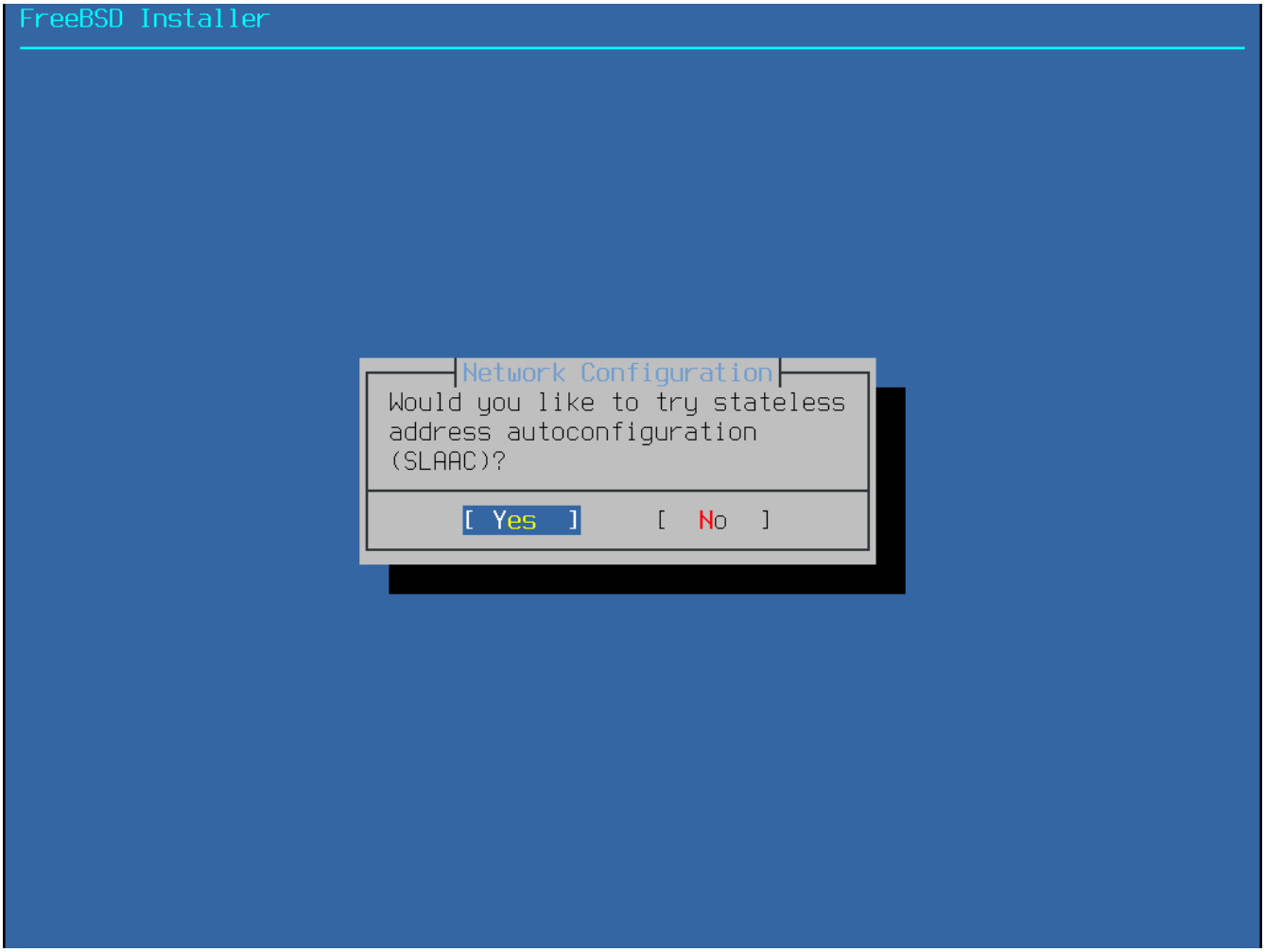


Σχήμα 28. Επιλογή Δικτύωσης IPv6

Το IPv6 διαθέτει επίσης δύο μεθόδους ρύθμισης. Το *SLAAC*, ή *StateLess Address AutoConfiguration*, ρυθμίζει αυτόματα τις παραμέτρους του δικτύου σας. Η ρύθμιση *Static* απαιτεί να κάνετε τις αντίστοιχες ρυθμίσεις χειροκίνητα.

4.9.2.3.1. IPv6 Stateless Address Autoconfiguration

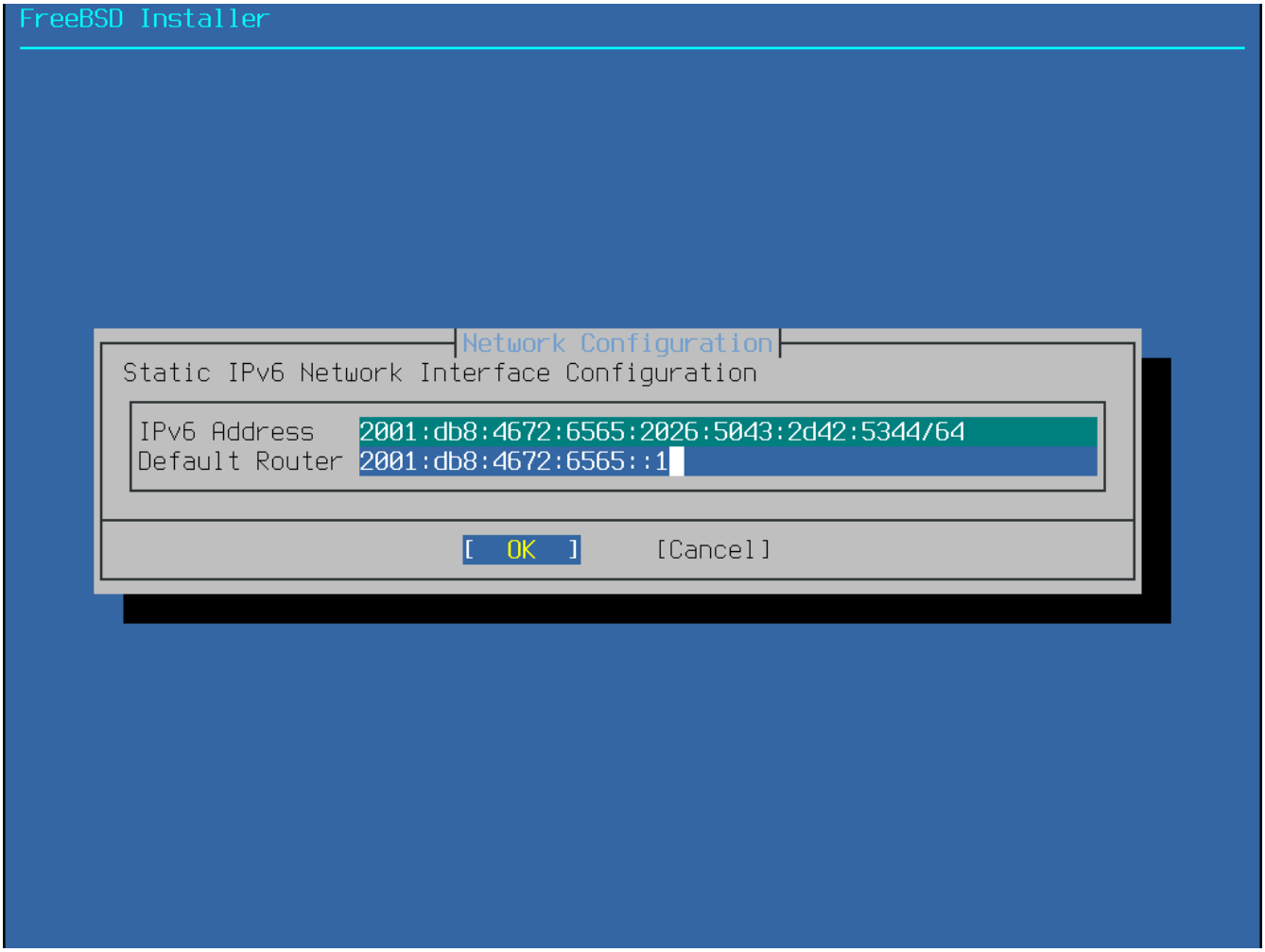
Το SLAAC επιτρέπει σε μια συσκευή ενός δικτύου IPv6 να ζητήσει πληροφορίες αυτόματης ρύθμισης από ένα τοπικό δρομολογητή. Δείτε το RFC4862 για περισσότερες πληροφορίες.



Σχήμα 29. Επιλέξτε Ρύθμιση IPv6 SLAAC

4.9.2.3.2. Στατική Ρύθμιση Δικτύου IPv6

Η στατική ρύθμιση της διεπαφής δικτύου στο IPv6, απαιτεί την χειροκίνητη εισαγωγή κάποιων ρυθμίσεων.

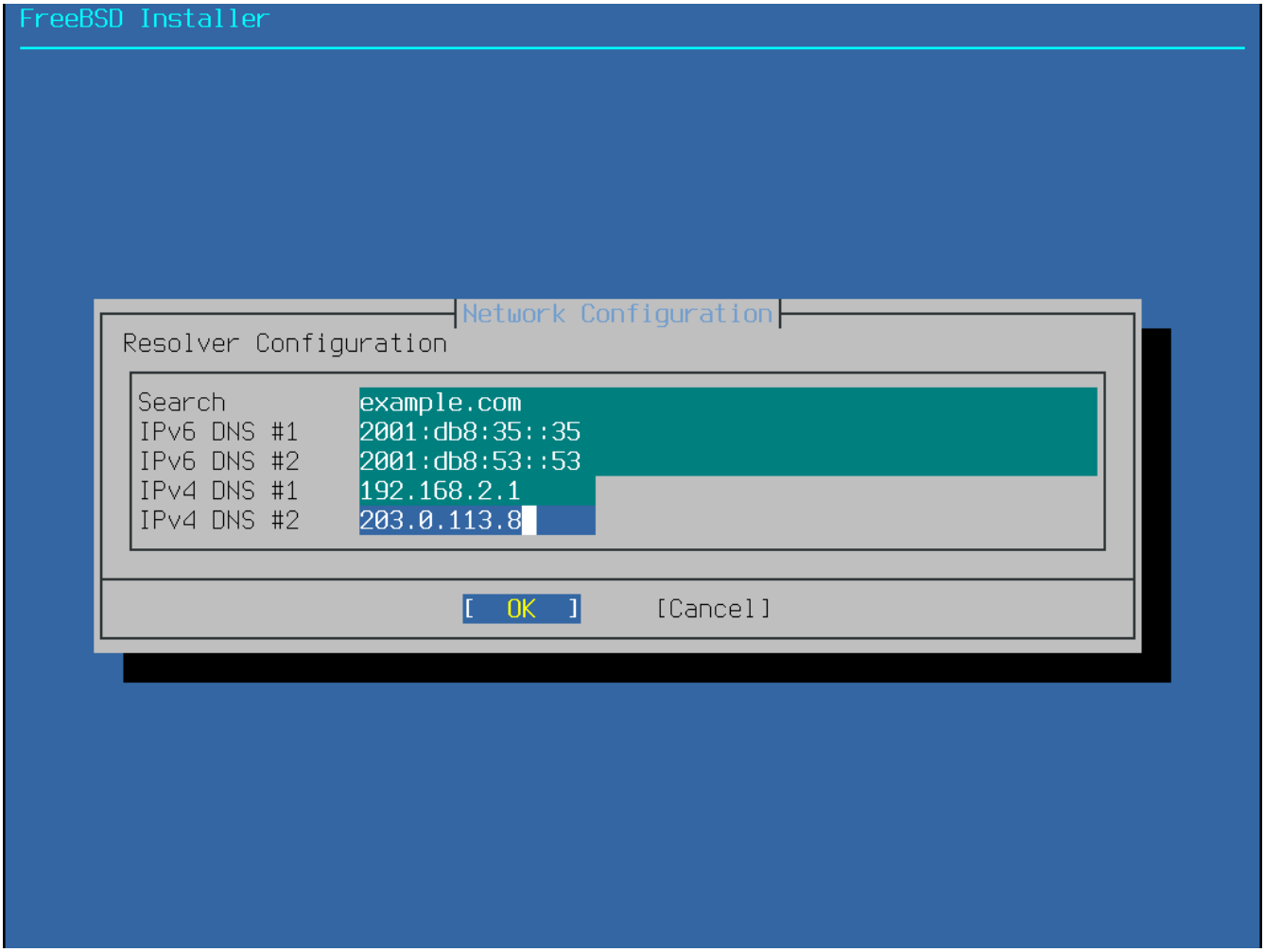


Σχήμα 30. Στατική Ρύθμιση IPv6

- `IPv6 Address` - Η διεύθυνση IP που θα εισάγετε χειροκίνητα σε αυτό τον υπολογιστή. Η διεύθυνση αυτή πρέπει να είναι μοναδική και να μην χρησιμοποιείται από κανένα άλλο μηχάνημα στο τοπικό σας δίκτυο.
- `Default Router` - Η IPv6 διεύθυνση του προεπιλεγμένου δρομολογητή για το δίκτυο σας. Συνήθως είναι η διεύθυνση του δρομολογητή ή άλλου δικτυακού εξοπλισμού που συνδέει το τοπικό σας δίκτυο με το Internet. Θα τη δείτε επίσης να αναφέρεται ως *default gateway (προεπιλεγμένη πύλη)*.

4.9.2.4. Ρύθμιση του DNS

Το *Domain Name System (Σύστημα Ονομάτων Τομέα)* ή *DNS* μετατρέπει ονόματα υπολογιστών σε διευθύνσεις δικτύου και το αντίθετο. Αν χρησιμοποιήσατε DHCP ή SLAAC για να ρυθμίσετε αυτόματα τη διεπαφή δικτύου, οι αντίστοιχες ρυθμίσεις πιθανόν να έχουν γίνει ήδη. Στην αντίθετη περίπτωση, βάλτε το όνομα τομέα του τοπικού δικτύου στο πεδίο Search. Τα πεδία DNS #1 και DNS #2 είναι οι διευθύνσεις IP των τοπικών εξυπηρετητών DNS. Χρειάζεται να εισάγετε τουλάχιστον ένα εξυπηρετητή DNS.



Σχήμα 31. Ρύθμιση DNS

4.9.3. Ρύθμιση της Ζώνης Ώρας

Η ρύθμιση της σωστής ζώνης ώρας στο μηχάνημα σας, εξασφαλίζει την αυτόματη αλλαγή της από χειμερινή σε εαρινή και το αντίστροφο. Επιτρέπει επίσης τη σωστή λειτουργία όλων των υπηρεσιών που σχετίζονται με την τήρηση χρόνου.

Το παράδειγμα μας αναφέρεται σε ένα μηχάνημα που βρίσκεται στην Ανατολική ζώνη ώρας των Ηνωμένων Πολιτειών. Η δική σας επιλογή θα είναι διαφορετική ανάλογα με τη γεωγραφική σας περιοχή.

Σχήμα 32. Επιλογή Τοπικού ή UTC Ρολογιού

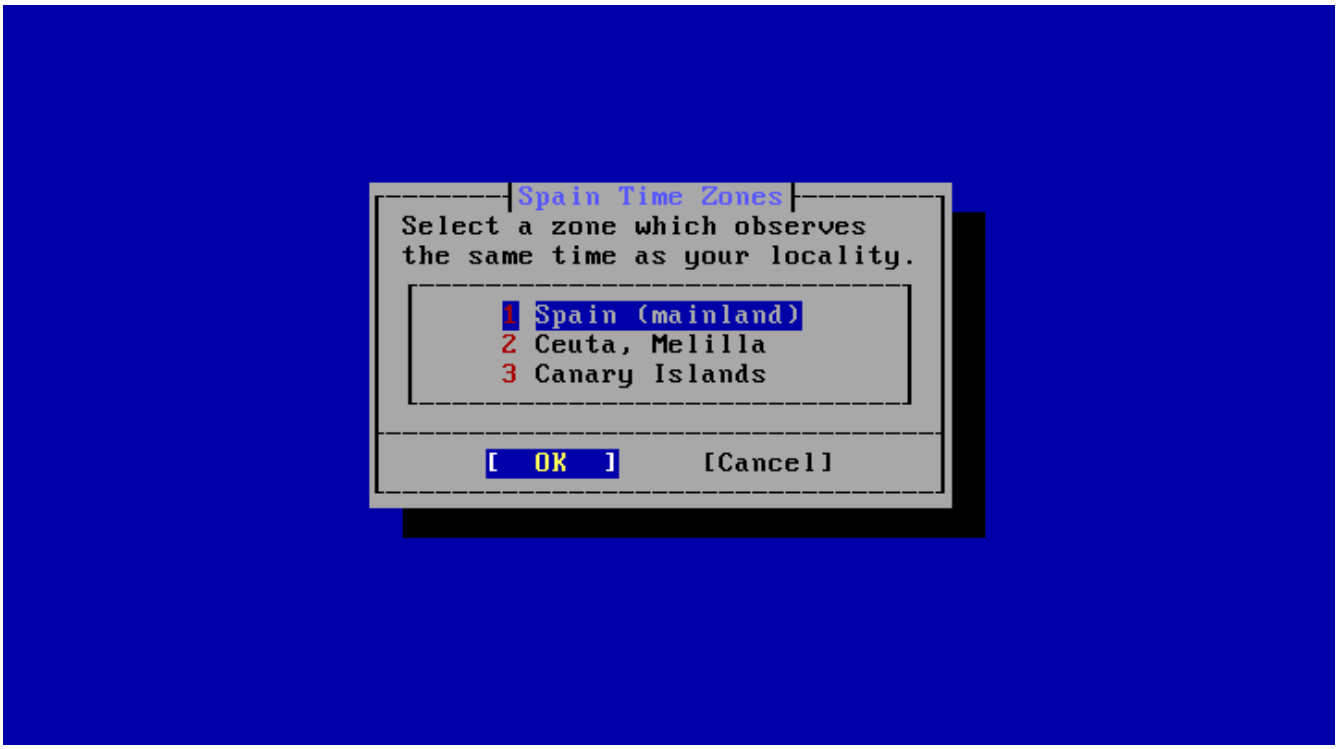
Επιλέξτε **[Yes]** ή **[No]** ανάλογα με το πως είναι ρυθμισμένο το ρολόι του μηχανήματος και πιέστε `Enter`. Αν δεν γνωρίζετε αν το σύστημα σας χρησιμοποιεί ώρα UTC ή τοπική, επιλέξτε **[No]** για να επιλέξετε την τοπική ώρα που είναι και η πιο συνηθισμένη.

Σχήμα 33. Επιλέξτε μια Περιοχή

Επιλέξτε την σωστή περιοχή χρησιμοποιώντας τα βελάκια και πιέστε `Enter`.

Σχήμα 34. Επιλογή Χώρας

Επιλέξτε τη σωστή χώρα χρησιμοποιώντας τα βελάκια και πιέστε `Enter`.



Σχήμα 35. Επιλογή Ζώνης Ώρας

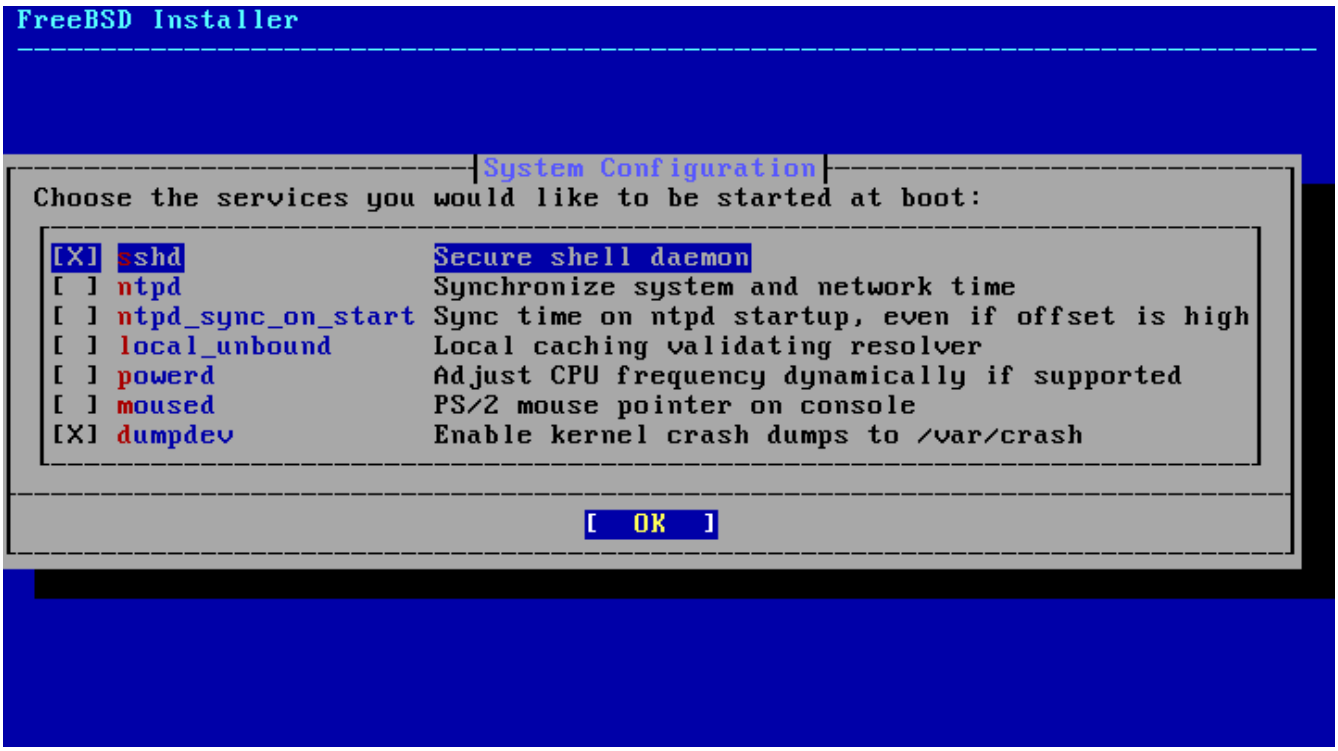
Επιλέξτε τη σωστή ζώνη ώρας χρησιμοποιώντας τα βελάκια και πιέστε `Enter`.

Σχήμα 36. Επιβεβαίωση Ζώνης Ώρας

Επιβεβαιώστε ότι η συντομογραφία για την επιλεγμένη ζώνη ώρας είναι η σωστή. Έπειτα πιέστε `Enter` για να συνεχίσετε με τις υπόλοιπες ρυθμίσεις.

4.9.4. Επιλογή Υπηρεσιών που θα Ενεργοποιηθούν

Μπορείτε να επιλέξετε ποιες από τις πρόσθετες υπηρεσίες θα ενεργοποιηθούν στην εκκίνηση. Όλες οι παρακάτω υπηρεσίες είναι προαιρετικές.



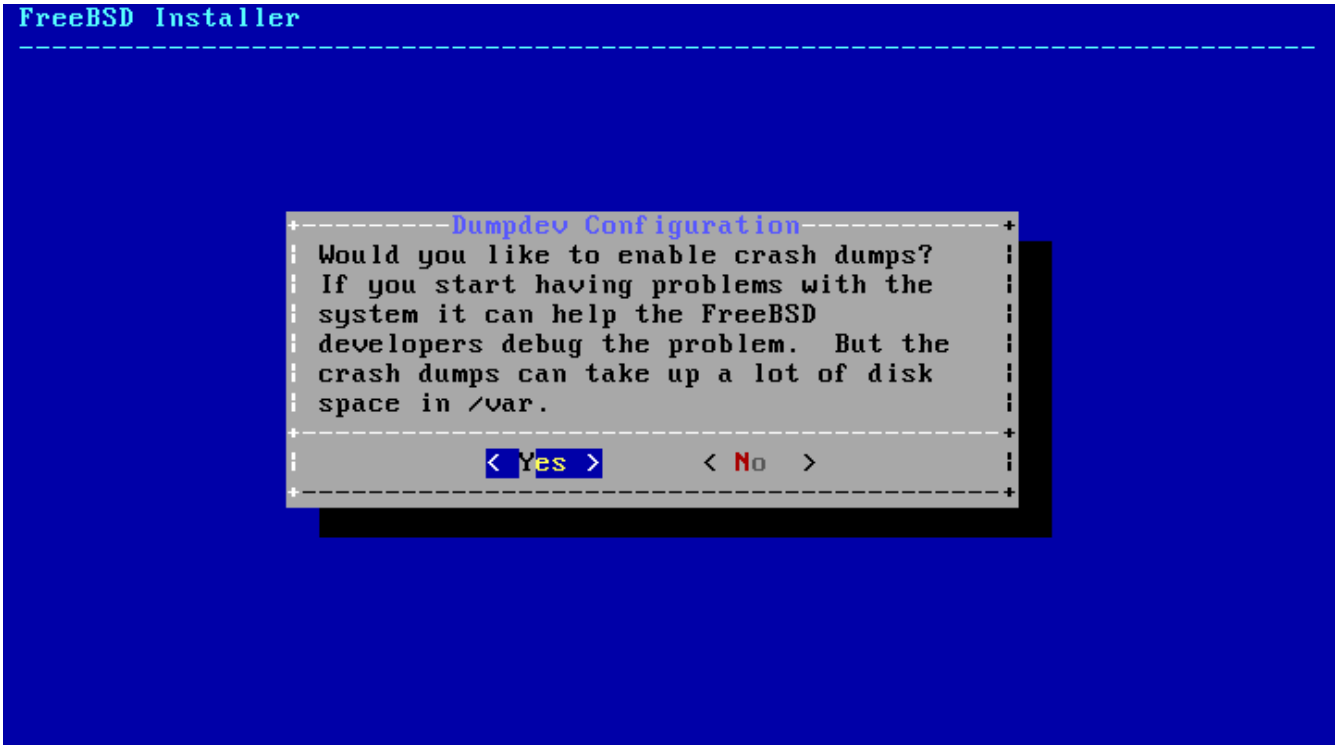
Σχήμα 37. Επιλογή Πρόσθετων Υπηρεσιών προς Ενεργοποίηση

Πρόσθετες Υπηρεσίες

- `sshd` - Secure Shell (Ασφαλές Κέλυφος) (SSH) Ο δαίμονας για ασφαλή απομακρυσμένη πρόσβαση.
- `moused` - Παρέχει δυνατότητα χρήσης του ποντικιού από την κονσόλα του συστήματος.
- `ntpd` - Network Time Protocol, πρωτόκολλο για ρύθμιση της ώρας μέσω δικτύου (NTP). Ο δαίμονας χρησιμοποιείται για την αυτόματη ρύθμιση του ρολογιού.
- `powerd` - Βοηθητικό πρόγραμμα για έλεγχο ισχύος και διαχείριση ενέργειας.

4.9.5. Ενεργοποίηση Crash Dumps

Το bsdinstall θα σας ρωτήσει αν θέλετε να ενεργοποιήσετε τα crash dumps στο σύστημα σας. Η ενεργοποίηση των crash dumps μπορεί να είναι πολύ χρήσιμη στον εντοπισμό προβλημάτων του συστήματος και για το λόγο αυτό συνιστούμε να τα ενεργοποιείτε όταν είναι δυνατόν. Επιλέξτε **[Yes]** για να τα ενεργοποιήσετε, ή **[No]** για να συνεχίσετε χωρίς crash dumps.



Σχήμα 38. Ενεργοποίηση Crash Dumps

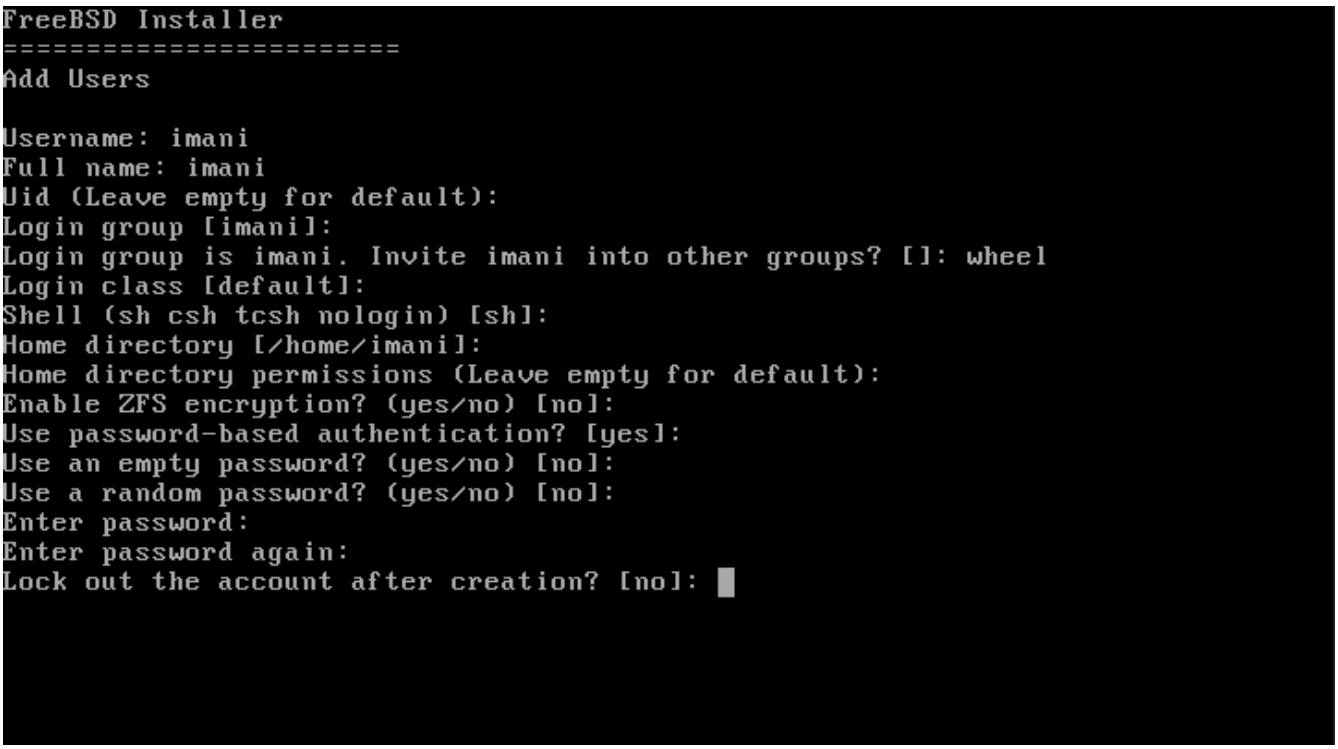
4.9.6. Προσθήκη Χρηστών

Η προσθήκη τουλάχιστον ενός χρήστη κατά την εγκατάσταση, σας επιτρέπει να χρησιμοποιήσετε το σύστημα χωρίς να εισέλθετε ως `root`. Όταν εισέρχεστε ως `root`, δεν υπάρχουν πρακτικά όρια ή κάποιο είδος προστασίας σχετικά με το τι μπορείτε να κάνετε. Όταν εισέρχεστε ως κανονικός χρήστης, μπορείτε να χειριστείτε το σύστημα σας με περισσότερη ασφάλεια.

Επιλέξτε **[Yes]** για να προσθέσετε νέους χρήστες.

Σχήμα 39. Προσθήκη Λογαριασμών Χρηστών

Εισάγετε τις πληροφορίες για το χρήστη που θα προστεθεί.



Σχήμα 40. Εισαγωγή Πληροφοριών Χρήστη

Πληροφορίες Χρήστη

- `Username` - Το όνομα που θα χρησιμοποιεί ο χρήστης για να εισέλθει στο σύστημα. Τυπικά το πρώτο γράμμα του μικρού ονόματος σε συνδυασμό με το επίθετο.
- `Full name` - Το πλήρες όνομα του χρήστη.
- `Uid` - User ID. Ο αναγνωριστικός αριθμός χρήστη. Συνήθως δεν συμπληρώνουμε αυτό το πεδίο, ώστε να επιλεγεί αυτόματα ένας αριθμός από το σύστημα.

- `Login group` - Η ομάδα στην οποία ανήκει ο χρήστης. Συνήθως το αφήνουμε κενό ώστε να γίνει αποδεκτή η προεπιλεγμένη τιμή.
- `Invite user into other groups?` - Επιπρόσθετες ομάδες χρηστών στις οποίες θέλουμε να ανήκει ο χρήστης.
- `Login class` - Συνήθως δεν συμπληρώνουμε αυτό το πεδίο, ώστε να γίνει αποδεκτή η προεπιλεγμένη τιμή.
- `Shell` - Το κέλυφος που θα χρησιμοποιεί ο συγκεκριμένος χρήστης. Στο παράδειγμα μας επιλέξαμε το csh(1).
- `Home directory` - Ο προσωπικός κατάλογος του χρήστη. Η προεπιλεγμένη τιμή είναι συνήθως η σωστή.
- `Home directory permissions` - Τα δικαιώματα στον κατάλογο του χρήστη. Τα προεπιλεγμένα είναι συνήθως σωστά.
- `Use password-based authentication?` - Η τυπική απάντηση είναι "yes".
- `Use an empty password?` - Η τυπική απάντηση είναι "no".
- `Use a random password?` - Η τυπική απάντηση είναι "no".
- `Enter password` - Ο κωδικός πρόσβασης για το συγκεκριμένο χρήστη. Δεν φαίνεται στην οθόνη καθώς τον πληκτρολογούμε.
- `Enter password again` - Ο κωδικός πρέπει να εισαχθεί άλλη μια φορά για επιβεβαίωση.
- `Lock out the account after creation?` - Η τυπική απάντηση είναι "no".

Αφού εισάγετε όλες τις πληροφορίες, θα δείτε μια περίληψη τους και το σύστημα θα σας ρωτήσει για την ορθότητα τους. Αν κάνατε κάποιο λάθος κατά τη διάρκεια της εισαγωγής, γράψτε `no` και ξαναπροσπαθήστε. Αν όλα είναι σωστά, γράψτε `yes` για να δημιουργήσετε το νέο χρήστη.

```
Login group [imani]:
Login group is imani. Invite imani into other groups? []: wheel
Login class [default]:
Shell (sh csh tcsh nologin) [sh]:
Home directory [/home/imani]:
Home directory permissions (Leave empty for default):
Enable ZFS encryption? (yes/no) [no]:
Use password-based authentication? [yes]:
Use an empty password? (yes/no) [no]:
Use a random password? (yes/no) [no]:
Enter password:
Enter password again:
Lock out the account after creation? [no]:
Username   : imani
Password   : *****
Full Name  : imani
Uid        : 1001
ZFS dataset : zroot/home/imani
Class      :
Groups     : imani wheel
Home       : /home/imani
Home Mode  :
Shell      : /bin/sh
Locked     : no
OK? (yes/no) [yes]:
```

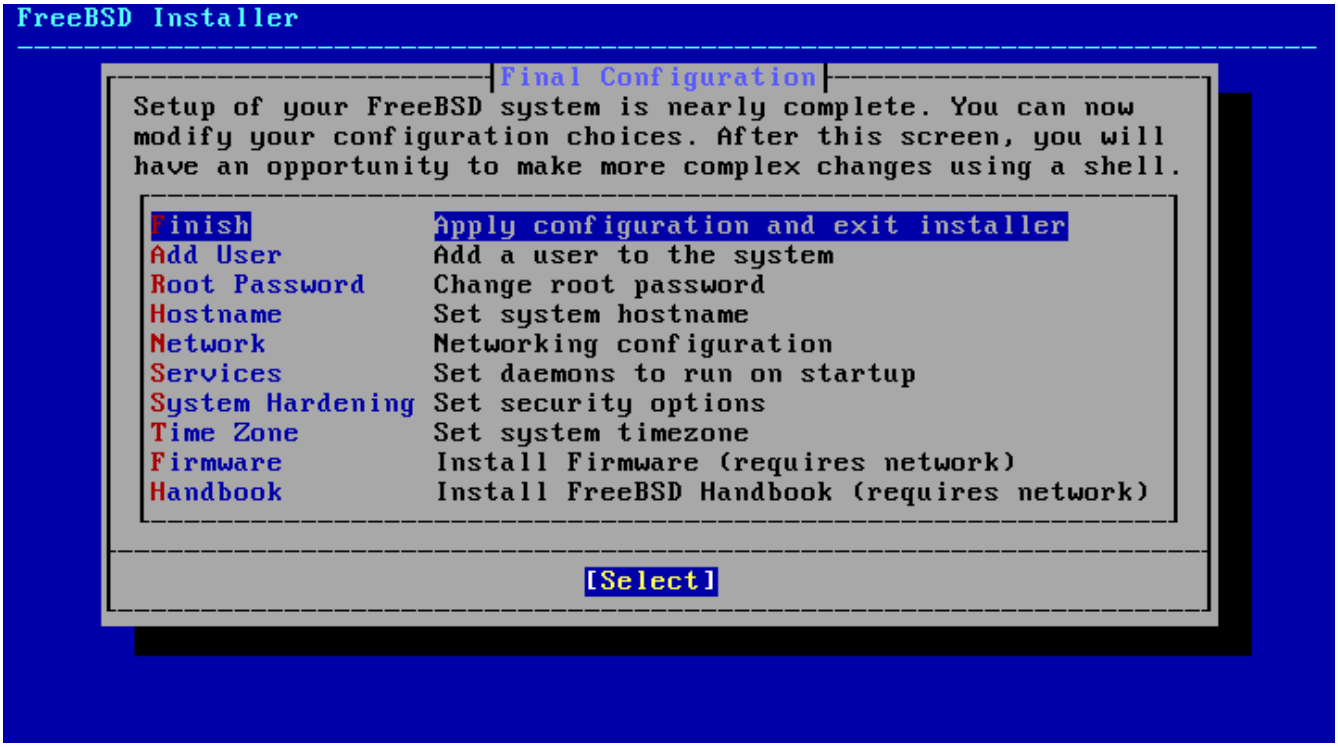
Σχήμα 41. Έξοδος από τη Διαχείριση Χρηστών και Ομάδων

Αν θέλετε να προσθέσετε περισσότερους χρήστες, απαντήστε στην ερώτηση "Add another user?" με `yes`. Απαντήστε `no` για να τελειώσετε με την προσθήκη χρηστών και να συνεχίσετε την εγκατάσταση.

Για περισσότερες πληροφορίες σχετικά με την προσθήκη και διαχείριση χρηστών, δείτε το Χρήστες και Βασική Διαχείριση Λογαριασμών.

4.9.7. Τελικές Ρυθμίσεις

Μετά το τέλος της εγκατάστασης και των αρχικών ρυθμίσεων, έχετε μια τελευταία ευκαιρία να αλλάξετε τις ρυθμίσεις πριν την έξοδο από το πρόγραμμα εγκατάστασης.



Σχήμα 42. Τελικές Ρυθμίσεις

Χρησιμοποιήστε αυτό το μενού για να κάνετε οποιεσδήποτε αλλαγές ή πρόσθετες ρυθμίσεις θέλετε πριν την ολοκλήρωση της εγκατάστασης.

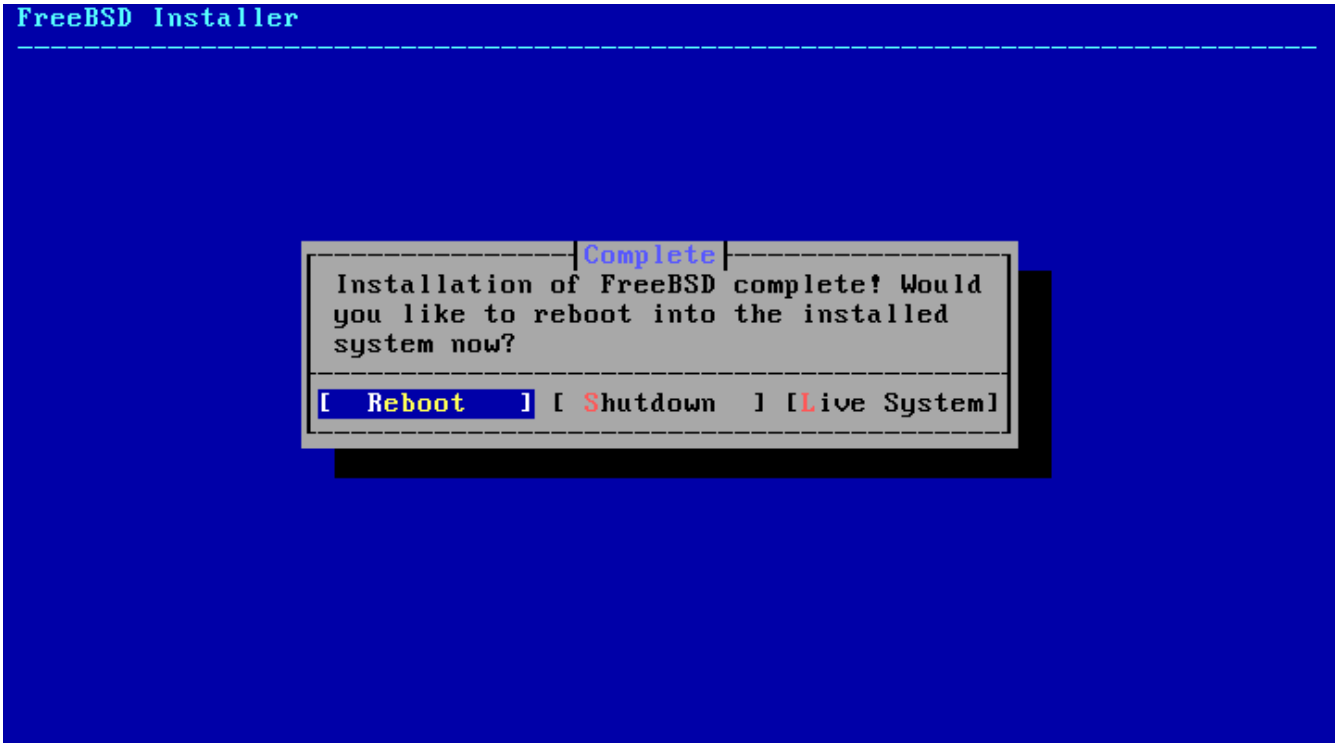
Επιλογές Τελικών Ρυθμίσεων

- `Add User` - Περιγράφεται στο Προσθήκη Χρηστών.
- `Root Password` - Περιγράφεται στο Ρύθμιση του Κωδικού του `root`.
- `Hostname` - Περιγράφεται στο Καθορισμός Ονόματος Υπολογιστή (hostname).
- `Network` - Περιγράφεται στο Ρύθμιση Καρτών Δικτύου.
- `Services` - Περιγράφεται στο Επιλογή Υπηρεσιών που θα Ενεργοποιηθούν.
- `Time Zone` - Περιγράφεται στο Ρύθμιση της Ζώνης Ώρας.
- `Handbook` - Μεταφόρτωση και εγκατάσταση του Εγχειριδίου του FreeBSD (το οποίο διαβάζετε αυτή τη στιγμή).

Με την ολοκλήρωση των τελικών ρυθμίσεων, επιλέξτε **[Exit]** για να κλείσετε την εγκατάσταση.

Σχήμα 43. Χειροκίνητη Ρύθμιση

Το bsdinstall θα σας ρωτήσει για τυχόν επιπλέον ρυθμίσεις που πρέπει να γίνουν πριν επανεκκινήσετε στο νέο σύστημα. Επιλέξτε **[Yes]** για να εκκινήσετε ένα κέλυφος στο νέο σύστημα ή **[No]** για να προχωρήσετε στο τελευταίο βήμα της εγκατάστασης.



Σχήμα 44. Ολοκλήρωση της Εγκατάστασης

Αν χρειάζεται να κάνετε περισσότερες ή ειδικές ρυθμίσεις, μπορείτε να επιλέξετε **[Live CD]**. Με την επιλογή αυτή, Θα ξεκινήσετε το μέσο εγκατάστασης σε κατάσταση Live CD.

Με την ολοκλήρωση της εγκατάστασης, επιλέξτε **[Reboot]** για να επανεκκινήσετε τον υπολογιστή σας και να ξεκινήσετε το νέο FreeBSD σύστημά σας. Μη ξεχάσετε να αφαιρέσετε το μέσο

εγκατάστασης από τον οδηγό CD (ή την USB υποδοχή), διαφορετικά το σύστημα σας ίσως ξεκινήσει ξανά από αυτό.

4.9.8. Εκκίνηση και Τερματισμός του FreeBSD

4.9.8.1. Εκκίνηση στο FreeBSD/i386

Κατά την εκκίνηση του FreeBSD εμφανίζονται πολλά πληροφοριακά μηνύματα. Φυσιολογικά, τα περισσότερα κυλούν εκτός της οθόνης. Μετά το τέλος της εκκίνησης εμφανίζεται η προτροπή εισόδου στο σύστημα (login). Μπορείτε να δείτε τα μηνύματα που κύλησαν εκτός οθόνης πιέζοντας το πλήκτρο `Scroll-Lock` για να να ενεργοποιήσετε την *προσωρινή μνήμη κύλισης*. Χρησιμοποιήστε έπειτα τα πλήκτρα `PgUp`, `PgDn` και τα βελάκια για να δείτε τα παλιά μηνύματα. Πιέζοντας το `Scroll-Lock` ξανά, θα επιστρέψετε στην κανονική απεικόνιση.

Στην προτροπή `login:` γράψτε το όνομα που δημιουργήσατε κατά την εγκατάσταση, στο παράδειγμα μας `asample`. Να αποφεύγετε να εισέρχεστε ως `root` όταν δεν είναι απαραίτητο.

Η δυνατότητα προς τα πίσω κύλισης των μηνυμάτων που περιγράψαμε προηγουμένως είναι περιορισμένη, επομένως δεν θα μπορέσετε με αυτό τον τρόπο να τα δείτε όλα. Μετά την είσοδο σας στο σύστημα, μπορείτε να δείτε τα μηνύματα από τη γραμμή εντολών γράφοντας `dmesg | less` στην προτροπή. Πιέστε `q` για να επιστρέψετε στη γραμμή εντολών όταν τελειώσετε.

Τυπικά μηνύματα εκκίνησης (έχουν παραλειφθεί οι πληροφορίες έκδοσης):

```
Copyright (c) 1992-2011 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.
FreeBSD is a registered trademark of The FreeBSD Foundation.

    root@farrell.cse.buffalo.edu:/usr/obj/usr/src/sys/GENERIC amd64
CPU: Intel(R) Core(TM)2 Duo CPU     E8400  @ 3.00GHz (3007.77-MHz K8-class CPU)
  Origin = "GenuineIntel"  Id = 0x10676  Family = 6  Model = 17  Stepping = 6
  Features
=0x783fbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PSE36,MMX
,FXSR,SSE,SSE2>
  Features2=0x209<SSE3,MON,SSSE3>
  AMD Features=0x20100800<SYSCALL,NX,LM>
  AMD Features2=0x1<LAHF>
real memory  = 536805376 (511 MB)
avail memory = 491819008 (469 MB)
Event timer "LAPIC" quality 400
ACPI APIC Table: <VBOX   VBOXAPIC>
ioapic0: Changing APIC ID to 1
ioapic0 <Version 1.1> irqs 0-23 on motherboard
kbd1 at kbdmux0
acpi0: <VBOX VBOXXSDT> on motherboard
acpi0: Power Button (fixed)
acpi0: Sleep Button (fixed)
Timecounter "ACPI-fast" frequency 3579545 Hz quality 900
acpi_timer0: <32-bit timer at 3.579545MHz> port 0x4008-0x400b on acpi0
```

```
cpu0: <ACPI CPU> on acpi0
pcib0: <ACPI Host-PCI bridge> port 0xcf8-0xcff on acpi0
pci0: <ACPI PCI bus> on pcib0
isab0: <PCI-ISA bridge> at device 1.0 on pci0
isa0: <ISA bus> on isab0
atapci0: <Intel PIIX4 UDMA33 controller> port 0x1f0-0x1f7,0x3f6,0x170-
0x177,0x376,0xd000-0xd00f at device 1.1 on pci0
ata0: <ATA channel 0> on atapci0
ata1: <ATA channel 1> on atapci0
vgapci0: <VGA-compatible display> mem 0xe0000000-0xe0ffffff irq 18 at device 2.0 on
pci0
em0: <Intel(R) PRO/1000 Legacy Network Connection 1.0.3> port 0xd010-0xd017 mem
0xf0000000-0xf001ffff irq 19 at device 3.0 on pci0
em0: Ethernet address: 08:00:27:9f:e0:92
pci0: <base peripheral> at device 4.0 (no driver attached)
pcm0: <Intel ICH (82801AA)> port 0xd100-0xd1ff,0xd200-0xd23f irq 21 at device 5.0 on
pci0
pcm0: <SigmaTel STAC9700/83/84 AC97 Codec>
ohci0: <OHCI (generic) USB controller> mem 0xf0804000-0xf0804fff irq 22 at device 6.0
on pci0
usbus0: <OHCI (generic) USB controller> on ohci0
pci0: <bridge> at device 7.0 (no driver attached)
acpi_acad0: <AC Adapter> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1 on acpi0
atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
atkbd0: [GIANT-LOCKED]
psm0: <PS/2 Mouse> irq 12 on atkbdc0
psm0: [GIANT-LOCKED]
psm0: model IntelliMouse Explorer, device ID 4
attimer0: <AT timer> port 0x40-0x43,0x50-0x53 on acpi0
Timecounter "i8254" frequency 1193182 Hz quality 0
Event timer "i8254" frequency 1193182 Hz quality 100
sc0: <System console> at flags 0x100 on isa0
sc0: VGA <16 virtual consoles, flags=0x300>
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff on isa0
atrtc0: <AT realtime clock> at port 0x70 irq 8 on isa0
Event timer "RTC" frequency 32768 Hz quality 0
ppc0: cannot reserve I/O port range
Timecounters tick every 10.000 msec
pcm0: measured ac97 link rate at 485193 Hz
em0: link state changed to UP
usbus0: 12Mbps Full Speed USB v1.0
ugen0.1: <Apple> at usbus0
uhub0: <Apple OHCI root HUB, class 9/0, rev 1.00/1.00, addr 1> on usbus0
cd0 at ata1 bus 0 scbus1 target 0 lun 0
cd0: <VBOX CD-ROM 1.0> Removable CD-ROM SCSI-0 device
cd0: 33.300MB/s transfers (UDMA2, ATAPI 12bytes, PIO 65534bytes)
cd0: Attempt to query device size failed: NOT READY, Medium not present
ada0 at ata0 bus 0 scbus0 target 0 lun 0
ada0: <VBOX HARDDISK 1.0> ATA-6 device
```

```
ada0: 33.300MB/s transfers (UDMA2, PIO 65536bytes)
ada0: 12546MB (25694208 512 byte sectors: 16H 63S/T 16383C)
ada0: Previously was known as ad0
Timecounter "TSC" frequency 3007772192 Hz quality 800
Root mount waiting for: usbus0
uhub0: 8 ports with 8 removable, self powered
Trying to mount root from ufs:/dev/ada0p2 [rw]...
Setting hostuuid: 1848d7bf-e6a4-4ed4-b782-bd3f1685d551.
Setting hostid: 0xa03479b2.
Entropy harvesting: interrupts ethernet point_to_point kickstart.
Starting file system checks:
/dev/ada0p2: FILE SYSTEM CLEAN; SKIPPING CHECKS
/dev/ada0p2: clean, 2620402 free (714 frags, 327461 blocks, 0.0% fragmentation)
Mounting local file systems:.
vboxguest0 port 0xd020-0xd03f mem 0xf0400000-0xf07fffff,0xf0800000-0xf0803fff irq 20
at device 4.0 on pci0
vboxguest: loaded successfully
Setting hostname: machine3.example.com.
Starting Network: lo0 em0.
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
        inet 127.0.0.1 netmask 0xff000000
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        options=9b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM>
        ether 08:00:27:9f:e0:92
        nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
        media: Ethernet autoselect (1000baseT <full-duplex>)
        status: active
Starting devd.
Starting Network: usbus0.
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 10.0.2.2
bound to 192.168.1.142 -- renewal in 43200 seconds.
add net ::ffff:0.0.0.0: gateway ::1
add net ::0.0.0.0: gateway ::1
add net fe80::: gateway ::1
add net ff02::: gateway ::1
ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/local/lib
32-bit compatibility ldconfig path: /usr/lib32
Creating and/or trimming log files.
Starting syslogd.
No core dumps found.
Clearing /tmp (X related).
Updating motd:.
Configuring syscons: blanktime.
Generating public/private rsa1 key pair.
Your identification has been saved in /etc/ssh/ssh_host_key.
Your public key has been saved in /etc/ssh/ssh_host_key.pub.
```

```
The key fingerprint is:
10:a0:f5:af:93:ae:a3:1a:b2:bb:3c:35:d9:5a:b3:f3 root@machine3.example.com
The key's randomart image is:
+--[RSA1 1024]----+
|    o..          |
|   o . .         |
|  .   o          |
|       o         |
|    o   S        |
|   + + o         |
|o . + *          |
|o+ ..+ .         |
|==o..o+E         |
+-----------------+
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
7e:1c:ce:dc:8a:3a:18:13:5b:34:b5:cf:d9:d1:47:b2 root@machine3.example.com
The key's randomart image is:
+--[ DSA 1024]----+
|       ..     . .|
|      o  .   . + |
|     . ..   . E .|
|    . .  o o . . |
|     +  S = .    |
|    +  . = o     |
|     +  . * .    |
|    . .  o .     |
|      .o. .      |
+-----------------+
Starting sshd.
Starting cron.
Starting background file system checks in 60 seconds.

Thu Oct  6 19:15:31 MDT 2011

FreeBSD/amd64 (machine3.example.com) (ttyv0)

login:
```

Η δημιουργία των κλειδιών RSA και DSA μπορεί να πάρει κάποιο χρόνο σε αργά μηχανήματα. Γίνεται όμως μόνο στην πρώτη εκκίνηση και μόνο αν έχει ρυθμιστεί το sshd για αυτόματη εκκίνηση. Οι επόμενες εκκινήσεις θα είναι ταχύτερες.

Το FreeBSD δεν εγκαθιστά κάποιο γραφικό περιβάλλον από προεπιλογή, αλλά υπάρχουν αρκετά διαθέσιμα προς εγκατάσταση. Δείτε το Το Σύστημα X Window για περισσότερες πληροφορίες.

4.9.9. Τερματισμός του FreeBSD

Ο σωστός τερματισμός του FreeBSD εξασφαλίζει τα δεδομένα και το υλικό του υπολογιστή σας από ζημιά. Δεν πρέπει απλώς να διακόψετε την τροφοδοσία. Αν ο χρήστης σας είναι μέλος της ομάδας `wheel`, μπορείτε να γίνετε υπερχρήστης με την εντολή `su` και την εισαγωγή του κωδικού του `root`. Διαφορετικά, συνδεθείτε ως `root` και χρησιμοποιήστε την εντολή `shutdown -p now`. Το σύστημα θα τερματίσει με το σωστό τρόπο και θα διακοπεί και η παροχή ρεύματος.

Μπορείτε να χρησιμοποιήσετε το συνδυασμό πλήκτρων `Ctrl` + `Alt` + `Del` για να επανεκκινήσετε το σύστημα, αλλά αυτό δεν συνίσταται κατά τη διάρκεια της κανονικής λειτουργίας.

4.10. Αντιμετώπιση Προβλημάτων

Η ενότητα που ακολουθεί καλύπτει την αντιμετώπιση βασικών προβλημάτων εγκατάστασης - για παράδειγμα κοινά προβλήματα που έχουν αναφερθεί από πολλούς χρήστες. Υπάρχουν επίσης κάποιες ερωτήσεις και απαντήσεις για όσους επιθυμούν να έχουν το FreeBSD ως dual boot με MS-DOS® ή Windows®.

4.10.1. Τι να Κάνετε αν Κάτι Πάει Στραβά

Λόγω των διάφορων περιορισμών στην αρχιτεκτονική του PC, δεν είναι δυνατόν η ανίχνευση συσκευών να είναι 100% αξιόπιστη. Υπάρχουν όμως κάποια πράγματα που μπορείτε να κάνετε αν η ανίχνευση δεν είναι επιτυχής.

Ελέγξτε τις Σημειώσεις Υλικού για την έκδοση του FreeBSD που χρησιμοποιείτε, για να βεβαιωθείτε ότι το υλικό σας υποστηρίζεται.

Αν το υλικό σας υποστηρίζεται και εξακολουθείτε να έχετε κολλήματα ή άλλα προβλήματα, θα πρέπει να δημιουργήσετε ένα προσαρμοσμένο πυρήνα. Αυτό θα σας επιτρέψει να προσθέσετε υποστήριξη για συσκευές οι οποίες δεν υπάρχουν στον πυρήνα GENERIC. Ο πυρήνας στο μέσο εγκατάστασης έχει δημιουργηθεί με την υπόθεση ότι οι περισσότερες συσκευές βρίσκονται στις προεπιλεγμένες ρυθμίσεις τους όσο αφορά τα IRQs, τις διευθύνσεις IO και τα κανάλια DMA. Αν έχετε αλλάξει αυτές τις ρυθμίσεις ίσως χρειαστεί να αλλάξετε τις ρυθμίσεις του πυρήνα και να τον επαναμεταγλωττίσετε για να μπορέσει το FreeBSD να εντοπίσει τις συσκευές σας.

Είναι επίσης πιθανό η διαδικασία ανίχνευσης για μια συσκευή που δεν είναι εγκατεστημένη να προκαλέσει πρόβλημα στην ανίχνευση μιας άλλης υπαρκτής συσκευής. Στην περίπτωση αυτή, θα πρέπει να αφαιρέσετε την ανίχνευση για τη συσκευή που δημιουργεί το πρόβλημα.

Κάποια προβλήματα εγκατάστασης μπορούν να αποφευχθούν ή να μειωθούν με την αναβάθμιση firmware διάφορων συσκευών υλικού και ειδικότερα της μητρικής. Το firmware της μητρικής είναι συχνά γνωστό με τον όρο BIOS. Οι περισσότεροι κατασκευαστές μητρικών διαθέτουν μια δικτυακή τοποθεσία από όπου μπορείτε να κατεβάσετε αναβαθμισμένες εκδόσεις και ανάλογες πληροφορίες.

Οι κατασκευαστές συνήθως συνιστούν να μην αναβαθμίζετε το BIOS της μητρικής αν δεν υπάρχει καλός λόγος, όπως για παράδειγμα μια κρίσιμη ενημέρωση. Η ενημέρωση *ενδέχεται να αποτύχει* αφήνοντας το BIOS σε μια ενδιάμεση κατάσταση

και τον υπολογιστή εκτός λειτουργίας.

4.10.2. Ερωτήσεις και Απαντήσεις στην Αντιμετώπιση Προβλημάτων

4.10.3. Το σύστημα μου σταματά να ανταποκρίνεται κατά την ανίχνευση συσκευών στην εκκίνηση ή συμπεριφέρεται περίεργα κατά την εγκατάσταση.

Το FreeBSD κάνει εκτεταμένη χρήση των υπηρεσιών ACPI (εφόσον υπάρχει) στις αρχιτεκτονικές i386, amd64 και ia64 ώστε να ρυθμίσει σωστά τις συσκευές κατά την εκκίνηση. Δυστυχώς υπάρχουν ακόμα κάποια προβλήματα τόσο στο ACPI όσο και στο BIOS firmware αρκετών μητρικών. Μπορείτε να απενεργοποιήσετε το ACPI θέτοντας `hint.acpi.0.disabled` στο τρίτο στάδιο του φορτωτή εκκίνησης:

```
set hint.acpi.0.disabled="1"
```

Καθώς η ρύθμιση αυτή χάνεται σε κάθε εκκίνηση, είναι απαραίτητο να προσθέσετε την οδηγία `hint.acpi.0.disabled="1"` στο αρχείο /boot/loader.conf. Μπορείτε να βρείτε περισσότερες πληροφορίες για το φορτωτή εκκίνησης στο Σύνοψη.

4.11. Χρησιμοποιώντας τη Λειτουργία Live CD

Η λειτουργία live CD του FreeBSD διατίθεται στο ίδιο CD με το βασικό πρόγραμμα εγκατάστασης. Είναι χρήσιμη για όσους ακόμα αναρρωτιούνται αν το FreeBSD είναι το κατάλληλο λειτουργικό για αυτούς και θέλουν να δοκιμάσουν κάποια από τα χαρακτηριστικά του πριν το εγκαταστήσουν.

Κατά τη χρήση του live CD να έχετε υπόψη σας τα παρακάτω:

- Για να αποκτήσετε πρόσβαση στο σύστημα θα πρέπει να περάσετε από διαδικασία εισόδου. Το όνομα χρήστη είναι `root` και ο κωδικός είναι κενός.
- Καθώς το σύστημα εκτελείται απευθείας από το CD, η απόδοση του θα είναι σημαντικά χαμηλότερη σε σχέση με ένα σύστημα εγκατεστημένο σε σκληρό δίσκο.
- Το live CD παρέχει μόνο γραμμή εντολών και όχι γραφικό περιβάλλον.

Chapter 5. Βασικές Έννοιες στο UNIX®

5.1. Σύνοψη

Το ακόλουθο κεφάλαιο θα καλύψει τις βασικές εντολές και λειτουργίες του λειτουργικού συστήματος FreeBSD. Το μεγαλύτερο μέρος αυτής της ύλης σχετίζεται με όλα τα Λ.Σ. που είναι βασισμένα στο UNIX®. Εάν η ύλη σας φαίνεται οικεία μπορείτε να διατρέξετε γρήγορα αυτό το κεφάλαιο. Εάν - αντιθέτως - είστε νέος στο FreeBSD τότε οπωσδήποτε θα πρέπει να διαβάσετε προσεκτικά ολόκληρο το κεφάλαιο.

Μετά την ανάγνωση του κεφαλαίου, θα γνωρίζετε:

- Πως να χρησιμοποιείτε τις "εικονικές κονσόλες" του FreeBSD.
- Πως λειτουργούν οι άδειες αρχείων στο UNIX® και θα καταλάβετε την χρήση των file flags στο FreeBSD.
- Την προεπιλεγμένη διάταξη του συστήματος αρχείων του FreeBSD.
- Την οργάνωση των δίσκων στο FreeBSD.
- Τι είναι και πώς λειτουργεί η προσάρτηση (mount) και αποπροσάρτηση (unmount) συστημάτων αρχείων.
- Τι είναι οι διεργασίες (processes), τα σήματα (signals) και οι δαίμονες (daemons).
- Τι είναι το κέλυφος (shell) και πως να αλλάζετε το προεπιλεγμένο περιβάλλον εργασίας.
- Πως να χρησιμοποιείτε βασικά προγράμματα επεξεργασίας κειμένου (editors).
- Τι είναι οι συσκευές (devices) και τα αρχεία συσκευής (device nodes).
- Ποια έκδοση εκτελέσιμων χρησιμοποιείται στο FreeBSD.
- Πως να διαβάζετε τις σελίδες βοηθείας (manual pages) για περισσότερες πληροφορίες.

5.2. Εικονικές Κονσόλες και Τερματικά

Μπορείτε να χειριστείτε το FreeBSD με διάφορους τρόπους. Ένας από αυτούς, είναι πληκτρολογώντας εντολές κειμένου σε ένα τερματικό. Με αυτό τον τρόπο έχετε στα χέρια σας ένα ευέλικτο και δυνατό λειτουργικό σύστημα UNIX®. Αυτή η ενότητα περιγράφει τι είναι τα "τερματικά" και οι "κονσόλες" και πως μπορούν να χρησιμοποιηθούν στο FreeBSD.

5.2.1. Η Κονσόλα

Εάν δεν έχετε ρυθμίσει το FreeBSD να ξεκινά αυτόματα κάποιο γραφικό περιβάλλον εργασίας, τότε αμέσως μετά την εκκίνηση του συστήματος και την ολοκλήρωση των σεναρίων εκκίνησης (startup scripts) θα εμφανιστεί η προτροπή σύνδεσης (login prompt). Θα δείτε κάτι παρόμοιο στην οθόνη σας:

```
Additional ABI support:.
Local package initialization:.
Additional TCP options:.
```

```
Fri Sep 20 13:01:06 EEST 2002

FreeBSD/i386 (pc3.example.org) (ttyv0)

login:
```

Το μήνυμα μπορεί να είναι λίγο διαφορετικό στο σύστημα σας, αλλά δεν πρέπει να διαφέρει κατά πολύ. Θα εστιάσουμε την προσοχή μας στις τελευταίες δύο γραμμές. Η προτελευταία γραμμή αναφέρει:

```
FreeBSD/i386 (pc3.example.org) (ttyv0)
```

Αυτή η γραμμή περιέχει μερικές πληροφορίες για το σύστημα που μόλις εκκινήσατε. Έχετε μπροστά σας μια κονσόλα "FreeBSD", που τρέχει με επεξεργαστή αρχιτεκτονικής x86 της Intel ή άλλον συμβατό . Το όνομα αυτής της μηχανής (όλες οι μηχανές UNIX® έχουν κάποιο όνομα) είναι `pc3.example.org`, και έχετε ανοικτό μπροστά σας το τερματικό ttyv0 - κονσόλα του συστήματος.

Ολοκληρώνοντας, η τελευταία γραμμή είναι πάντα:

```
login:
```

Σε αυτό το μέρος θα πρέπει να πληκτρολογήσετε το "όνομα χρήστη" (username) για να συνδεθείτε στο FreeBSD. Στην επόμενη ενότητα θα περιγράψουμε ακριβώς αυτήν την διαδικασία.

5.2.2. Εισαγωγή Χρήστη στο Σύστημα FreeBSD

Το FreeBSD είναι ένα σύστημα πολυχρηστικό (multiuser) και πολυεπεξεργαστικό (multiprocessing). Αυτός είναι ο ακαδημαϊκός ορισμός που δίνεται συνήθως σε ένα σύστημα που μπορεί να χρησιμοποιείται από πολλούς διαφορετικούς ανθρώπους, ενώ ταυτόχρονα τρέχουν διαφορετικά προγράμματα στην ίδια μηχανή.

Κάθε σύστημα multiuser χρειάζεται κάποιους τρόπους ώστε να ξεχωρίζει κάθε "χρήστη" από τους υπολοίπους. Στο FreeBSD (όπως και σε όλα τα Λ.Σ. που βασίζονται στο UNIX®), αυτό επιτυγχάνεται απαιτώντας κάθε χρήστης να "είναι συνδεδεμένος (log in)" πριν να μπορεί να τρέξει προγράμματα. Κάθε χρήστης έχει ξεχωριστό όνομα (το "όνομα χρήστη ή username") και μία προσωπική δικλείδα ασφαλείας, (τον "κωδικό πρόσβασης ή password"). Αυτά θα ζητηθούν από το FreeBSD σε κάθε χρήστη πριν να του επιτραπεί να τρέξει οποιαδήποτε εφαρμογή.

Αμέσως μετά την ολοκλήρωση των διεργασιών εκκίνησης του FreeBSD και των σεναρίων εκκίνησης (startup scripts) , θα εμφανιστεί το σύμβολο της προτροπής (prompt) και θα σας ζητηθεί ένα έγκυρο όνομα χρήστη:

```
login:
```

Για παράδειγμα, ας υποθέσουμε πως το όνομα χρήστη σας είναι `john`. Πληκτρολογήστε `john` στην

προτροπή και πατήστε `Enter`. Θα ακολουθήσει μια νέα προτροπή για να δώσετε τον "κωδικό πρόσβασης (password)":

```
login: john
Password:
```

Πληκτρολογήστε τώρα τον κωδικό πρόσβασης του `john`, και πατήστε `Enter`. Ο κωδικός πρόσβασης *δεν είναι ορατός!* Δεν χρειάζεται να ανησυχείτε για αυτό. Είναι επαρκές να πούμε πως αυτό συμβαίνει για λόγους ασφαλείας.

Αν έχετε πληκτρολογήσει σωστά τον κωδικό πρόσβασης, τότε έχετε συνδεθεί στο FreeBSD και είστε έτοιμοι να δοκιμάσετε όλες τις διαθέσιμες εντολές UNIX®.

Πρέπει να δείτε το MOTD ή αλλιώς το ημερήσιο μήνυμα και στη συνέχεια την προτροπή εντολής (ένα χαρακτήρα `#`, `$`, ή `%`). Αυτό σημαίνει πως έχετε συνδεθεί επιτυχώς στο FreeBSD.

5.2.3. Πολλαπλές Κονσόλες

Η εκτέλεση εντολών UNIX® σε μία μόνο κονσόλα μπορεί να είναι ικανοποιητική, αλλά το FreeBSD μπορεί να τρέχει ταυτόχρονα πολλά προγράμματα. Η ύπαρξη μίας μόνο κονσόλας για πληκτρολόγηση εντολών θα ήταν πραγματικά ελλιπής για ένα Λ.Σ. όπως το FreeBSD που μπορεί να τρέχει ταυτόχρονα δεκάδες προγράμματα. Εδώ είναι που χρειάζονται οι "εικονικές κονσόλες".

Το FreeBSD μπορεί να ρυθμιστεί κατάλληλα ώστε να παρουσιάζεται με διάφορες εικονικές κονσόλες. Η εναλλαγή από μία εικονική κονσόλα σε οποιαδήποτε άλλη μπορεί να γίνει πατώντας μερικά πλήκτρα στο πληκτρολόγιο. Η κάθε κονσόλα έχει το δικό της κανάλι εξόδου, και καθώς εναλλάσσετε εικονικές κονσόλες το FreeBSD αποθηκεύει και επαναφέρει προσεκτικά το αντίστοιχο πληκτρολόγιο και οθόνη για κάθε κονσόλα σαν να υπήρχε πραγματική εναλλαγή.

Συνδυασμοί ειδικών πλήκτρων χρησιμοποιούνται από το FreeBSD για την εναλλαγή κονσολών . Μπορείτε να χρησιμοποιήσετε `Alt` + `F1`, `Alt` + `F2`, έως `Alt` + `F8` για να μεταβείτε στις διάφορες εικονικές κονσόλες του FreeBSD.

Καθώς εναλλάσσεστε από τη μία κονσόλα στην άλλη, το FreeBSD αποθηκεύει και επαναφέρει προσεκτικά την αντίστοιχη οθόνη. Το αποτέλεσμα είναι ένα "οπτικό τρικ" σαν να είχαμε πολλαπλές "εικονικές" οθόνες και πληκτρολόγια που θα μπορούσαμε να χρησιμοποιήσουμε για να τρέχουμε εντολές στο FreeBSD. Τα προγράμματα που τρέχετε από μια κονσόλα δεν σταματούν να λειτουργούν όταν η κονσόλα δεν είναι ορατή. Συνεχίζουν να τρέχουν κι όταν βρίσκεστε σε διαφορετική κονσόλα.

5.2.4. Το Αρχείο /etc/ttys

Η εξ' ορισμού ρύθμιση του FreeBSD θα ξεκινήσει με οκτώ εικονικές κονσόλες. Δεν πρόκειται για μια πολύπλοκη ρύθμιση και μπορείτε εύκολα να την αλλάξετε ώστε να φορτώνονται περισσότερες ή λιγότερες εικονικές κονσόλες κατά την εκκίνηση. Το πλήθος και η παραμετροποίηση των εικονικών κονσολών ρυθμίζεται στο αρχείο /etc/ttys.

Μπορείτε να χρησιμοποιήσετε το αρχείο /etc/ttys για να ρυθμίσετε τις εικονικές κονσόλες στο FreeBSD. Κάθε γραμμή του αρχείου που δεν είναι σχόλιο (οι γραμμές που δεν ξεκινούν με τον

χαρακτήρα #) περιέχουν ρυθμίσεις για ένα τερματικό ή για μια εικονική κονσόλα. Η προκαθορισμένη έκδοση του αρχείου, η οποία περιέχεται στην διανομή FreeBSD, περιέχει εννέα εικονικές κονσόλες, εκ των οποίων οι οκτώ είναι ενεργοποιημένες. Είναι στις γραμμές που ξεκινούν με ttyv:

```
# name  getty                           type    status          comments
#
ttyv0   "/usr/libexec/getty Pc"         cons25  on  secure
# Virtual terminals
ttyv1   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv2   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv3   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv4   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv5   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv6   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv7   "/usr/libexec/getty Pc"         cons25  on  secure
ttyv8   "/usr/X11R6/bin/xdm -nodaemon"  xterm   off secure
```

Για μια λεπτομερή περιγραφή κάθε στήλης του αρχείου και όλων των ρυθμίσεων που μπορούν να εφαρμοστούν για τις εικονικές κονσόλες συμβουλευτείτε την σελίδα βοηθείας ttys(5).

5.2.5. Κονσόλα σε Κατάσταση Ενός Χρήστη

Μπορείτε να βρείτε μια λεπτομερή περιγραφή για το τι είναι "κατάσταση ενός χρήστη" στην ενότητα Κατάσταση Λειτουργίας Ενός Χρήστη. Αξίζει να αναφέρουμε πως υπάρχει ενεργή μόνο μία κονσόλα όταν τρέχετε το FreeBSD σε κατάσταση ενός χρήστη. Δεν υπάρχουν διαθέσιμες εικονικές κονσόλες. Στο αρχείο /etc/ttys μπορείτε να βρείτε τις ρυθμίσεις σε κατάσταση ενός χρήστη. Αναζητήστε την γραμμή που ξεκινά με console:

```
# name  getty                           type    status          comments
#
# If console is marked "insecure", then init will ask for the root password
# when going to single-user mode.
console none                            unknown off secure
```

Όπως αναφέρουν τα σχόλια πάνω από το console, μπορείτε να επεξεργαστείτε αυτήν τη γραμμή και να αντικαταστήσετε την λέξη secure με insecure. Σε αυτή την περίπτωση κατά την εκκίνηση του FreeBSD σε κατάσταση ενός χρήστη, θα σας ζητηθεί ο κωδικός πρόσβασης του υπερχρήστη root.

Προσέχετε όταν κάνετε την μετατροπή σε insecure. Εάν τύχει να ξεχάσετε τον κωδικό πρόσβασης του root, η πρόσβαση σε κατάσταση λειτουργίας ενός χρήστη μπορεί να γίνει δύσβατη. Υπάρχει ακόμη τρόπος να κάνετε εκκίνηση, αλλά ίσως να είναι δύσκολο για κάποιον που δεν γνωρίζει πολλά για τις διεργασίες και τα προγράμματα εκκίνησης του FreeBSD.

5.2.6. Αλλάζοντας την Ανάλυση (video mode) της Κονσόλας

Η προεπιλεγμένη απεικόνιση της κονσόλας στο FreeBSD μπορεί να ρυθμιστεί σε ανάλυση 1024x768, 1280x1024, ή σε οποιοδήποτε άλλο μέγεθος υποστηρίζεται από την κάρτα γραφικών και την οθόνη σας. Για να χρησιμοποιήσετε διαφορετική ανάλυση, θα πρέπει πρώτα από όλα να επαναμεταγλωττίσετε τον πυρήνα σας, και να συμπεριλάβετε τις παρακάτω δύο επιλογές:

```
options VESA
options SC_PIXEL_MODE
```

Μετά τη μεταγλώττιση του πυρήνα με τις παραπάνω δύο επιλογές, μπορείτε να βρείτε ποιες αναλύσεις υποστηρίζονται από το υλικό σας, χρησιμοποιώντας το βοηθητικό πρόγραμμα vidcontrol(1). Για να δείτε μια λίστα από τις υποστηριζόμενες αναλύσεις, δώστε την ακόλουθη εντολή:

```
# vidcontrol -i mode
```

Η έξοδος της εντολής αυτής, είναι μια λίστα από αναλύσεις οθόνης που υποστηρίζονται από το υλικό σας. Μπορείτε έπειτα να επιλέξετε μια νέα ανάλυση, δίνοντας την ως όρισμα στην vidcontrol(1) σε μια κονσόλα που έχετε συνδεθεί ως `root`:

```
# vidcontrol MODE_279
```

Αν η νέα ανάλυση γίνει δεκτή, μπορείτε να την ορίσετε ως προεπιλεγμένη για κάθε εκκίνηση, με την κατάλληλη ρύθμιση στο αρχείο /etc/rc.conf:

```
allscreens_flags="MODE_279"
```

5.3. Άδειες (Permissions)

Το FreeBSD είναι απόγονος του BSD UNIX®, και για αυτό το λόγο βασίζεται σε μερικές έννοιες κλειδιά του UNIX®. Η πρώτη και πιο σημαντική είναι πως το FreeBSD είναι ένα πολυχρηστικό (multiuser) λειτουργικό σύστημα. Το σύστημα μπορεί να εξυπηρετήσει πολλούς χρήστες που εργάζονται ταυτόχρονα και σε εντελώς ανεξάρτητες εφαρμογές. Το σύστημα είναι υπεύθυνο για τον σωστό διαμοιρασμό και τις ανάγκες διαχείρισης συσκευών hardware, περιφερειακών, μνήμης, και την σωστή κατανομή των πόρων της CPU για κάθε χρήστη.

Επειδή το σύστημα έχει την ικανότητα να εξυπηρετεί πολλούς χρήστες, σε οτιδήποτε διαχειρίζεται, υπάρχει μια ομάδα αδειών που ορίζει ποιος μπορεί να διαβάσει, να γράψει και να εκτελέσει αυτούς τους πόρους. Οι άδειες αποθηκεύονται σε οκτάδες διαχωρισμένες σε τρία μέρη, ένα για τον ιδιοκτήτη του αρχείου, ένα για την ομάδα στην οποία ανήκει το αρχείο, και ένα μέρος για όλους τους άλλους. Στη συνέχεια παρουσιάζεται πίνακας με τις αντιστοιχίες μεταξύ των ομάδων αδειών και των αριθμητικών τους τιμών.

Τιμή	Άδεια	Εμφάνιση σε περιεχόμενα καταλόγων
0	Ανάγνωση:όχι, Εγγραφή:όχι, Εκτέλεση:όχι	`---`
1	Ανάγνωση:όχι, Εγγραφή:όχι, Εκτέλεση:ναι	`--x`
2	Ανάγνωση:όχι, Εγγραφή:ναι, Εκτέλεση:όχι	`-w-`
3	Ανάγνωση:όχι, Εγγραφή:ναι, Εκτέλεση:ναι	`-wx`
4	Ανάγνωση:ναι, Εγγραφή:όχι, Εκτέλεση:όχι	`r--`
5	Ανάγνωση:ναι, Εγγραφή:όχι, Εκτέλεση:ναι	`r-x`
6	Ανάγνωση:ναι, Εγγραφή:ναι, Εκτέλεση:όχι	`rw-`
7	Ανάγνωση:ναι, Εγγραφή:ναι, Εκτέλεση:ναι	`rwx`

Μπορείτε να χρησιμοποιήσετε την εντολή ls(1) με πρόθεμα `-l` στην γραμμή εντολών για να δείτε τα περιεχόμενα καταλόγου και παρατηρήστε πως περιέχεται μια στήλη με τις άδειες των αρχείων για τον ιδιοκτήτη, την ομάδα, και για όλους τους άλλους. Για παράδειγμα, αν δώσουμε `ls -l` σε ένα τυχαίο κατάλογο:

```
% ls -l
total 530
-rw-r--r--  1 root  wheel     512 Sep  5 12:31 myfile
-rw-r--r--  1 root  wheel     512 Sep  5 12:31 otherfile
-rw-r--r--  1 root  wheel    7680 Sep  5 12:31 email.txt
...
```

Η πρώτη στήλη που παίρνουμε με την εντολή `ls -l` διαχωρίζεται ως εξής:

```
-rw-r--r--
```

Ο πρώτος χαρακτήρας (από τα αριστερά) μας ενημερώνει αν πρόκειται για ένα κανονικό αρχείο, κατάλογο, ειδική συσκευή χαρακτήρων, υποδοχέα (socket), ή οποιαδήποτε άλλο αρχείο ψευδο-συσκευής. Στην περίπτωση μας, το `-` υποδηλώνει ένα κανονικό αρχείο. Οι ακόλουθοι τρεις χαρακτήρες, στο παράδειγμα μας, `rw-`, ορίζουν τις άδειες για τον ιδιοκτήτη του αρχείου. Οι τρεις επόμενοι χαρακτήρες, `r--`, ορίζουν τις άδειες για την ομάδα στην οποία ανήκει το αρχείο. Οι τελευταίοι τρεις χαρακτήρες, `r--`, ορίζουν τις άδειες για τον υπόλοιπο κόσμο. Η παύλα σημαίνει πως η άδεια είναι απενεργοποιημένη. Στην περίπτωση του αρχείου μας, οι άδειες έχουν οριστεί ώστε ο ιδιοκτήτης να μπορεί να διαβάζει και να γράφει στο αρχείο, η ομάδα να μπορεί να διαβάσει το

αρχείο, και ο υπόλοιπος κόσμος να μπορεί μόνο να διαβάσει το αρχείο. Σύμφωνα με τον παραπάνω πίνακα, οι άδειες για αυτό το αρχείο είναι 644, όπου καθένα από τα τρία ψηφία παρουσιάζει το αντίστοιχο μέρος αδειών του αρχείου.

Μέχρι εδώ είναι όλα καλά, αλλά όμως πως το σύστημα ελέγχει τις άδειες συσκευών; Το FreeBSD μεταχειρίζεται τις περισσότερες συσκευές σαν ένα αρχείο το οποίο τα προγράμματα μπορούν να ανοίξουν, να διαβάσουν και να γράψουν σε αυτό σαν να ήταν ένα οποιοδήποτε αρχείο. Αυτά τα ειδικά αρχεία συσκευών αποθηκεύονται στον κατάλογο /dev.

Το σύστημα μεταχειρίζεται επίσης και τους καταλόγους ως αρχεία. Έχουν άδειες ανάγνωσης, εγγραφής και εκτέλεσης. Το bit που ορίζει την εκτέλεση στους καταλόγους έχει ελαφρώς διαφορετικό νόημα από ότι στα αρχεία. Όταν ένας κατάλογος έχει οριστεί εκτελέσιμος, σημαίνει πως είναι προσπελάσιμος, δηλαδή είναι επιτρεπτό να περάσουμε σε ένα υποκατάλογο του (να κάνουμε "cd"). Αυτό επίσης σημαίνει πως επιτρέπεται η πρόσβαση σε όλα τα γνωστά (αυτό έχει να κάνει με τις άδειες των ίδιων των αρχείων) αρχεία.

Ειδικότερα, για να εμφανίζονται τα περιεχόμενα καταλόγου πρέπει να έχει τεθεί άδεια ανάγνωσης (read) στον κατάλογο, ενώ για να διαγραφεί ένα αρχείο του οποίου γνωρίζετε το όνομα είναι αναγκαίο να έχουν δοθεί οι άδειες εγγραφής (write) *και* εκτέλεσης (execute) στον κατάλογο που περιέχει το αρχείο.

Υπάρχουν κι άλλα bit αδειών, αλλά χρησιμοποιούνται κυρίως σε ειδικές περιπτώσεις όπως σε setuid binaries και sticky directories. Αν θέλετε περισσότερες πληροφορίες για τις άδειες αρχείων και πως να τις ορίζετε, συμβουλευτείτε οπωσδήποτε την σελίδα manual chmod(1).

5.3.1. Συμβολικές Άδειες

Οι συμβολικές άδειες, μερικές φορές αναφέρονται και ως συμβολικές εκφράσεις, χρησιμοποιούν χαρακτήρες στην θέση των οκτώ τιμών για να θέτουν άδειες σε αρχεία ή καταλόγους. Οι συμβολικές εκφράσεις χρησιμοποιούν την σύνταξη (ποιος) (ενέργεια) (άδειες), όπου είναι διαθέσιμες οι ακόλουθες τιμές:

Επιλογή	Γράμμα	Σημαίνει
(ποιος)	u	User (Χρήστης)
(ποιος)	g	Group owner (Ομάδα που ανήκει)
(ποιος)	o	Other (Υπόλοιποι χρήστες)
(ποιος)	a	All (όλοι, "world")
(ενέργεια)	+	Πρόσθεση αδειών
(ενέργεια)	-	Αφαίρεση αδειών
(ενέργεια)	=	Άμεσος ορισμός αδειών
(άδειες)	r	Read (Ανάγνωση)
(άδειες)	w	Write (Εγγραφή)
(άδειες)	x	Execute (Εκτέλεση)

Επιλογή	Γράμμα	Σημαίνει
(άδειες)	t	Sticky bit
(άδειες)	s	Set UID ή GID

Οι τιμές εισάγονται με την εντολή chmod(1) όπως πριν, αλλά με γράμματα. Για παράδειγμα, θα μπορούσατε να χρησιμοποιήσετε την ακόλουθη εντολή για να απαγορεύσετε σε άλλους χρήστες την πρόσβαση στο *FILE*:

```
% chmod go= FILE
```

Μπορούν να γίνουν πάνω από μία αλλαγές στις άδειες ενός αρχείου ταυτόχρονα διαχωρίζοντας τις αλλαγές με κόμμα. Για παράδειγμα, η ακόλουθη εντολή θα αφαιρέσει στην ομάδα και στον "υπόλοιπο κόσμο" την άδεια εγγραφής, και στη συνέχεια θα προσθέσει άδεια εκτέλεσης σε όλους.

```
% chmod go-w,a+x FILE
```

5.3.2. FreeBSD File Flags

Πέρα από τις άδειες αρχείων που συζητήθηκαν πριν από λίγο, το FreeBSD υποστηρίζει την χρήση των "file flags." Αυτά τα flags προσθέτουν ένα επιπρόσθετο επίπεδο ασφαλείας και ελέγχου σε αρχεία, αλλά όχι σε καταλόγους.

Αυτά τα flags προσθέτουν ένα πρόσθετο επίπεδο ελέγχου σε αρχεία, διασφαλίζοντας μας πως σε κάποιες περιπτώσεις ακόμη κι ο `root` να μην μπορεί να διαγράψει ή να μετατρέψει αρχεία.

Η μετατροπή των file flags γίνεται με την chflags(1), χρησιμοποιώντας μια απλή διασύνδεση. Για παράδειγμα, για να ενεργοποιήσουμε το flag του συστήματος μη διαγραφής αρχείου στο αρχείο file1, δίνουμε την ακόλουθη εντολή:

```
# chflags sunlink file1
```

Για να απενεργοποιήσουμε το flag του συστήματος μη διαγραφής αρχείου, απλά δίνουμε την προηγούμενη εντολή με "no" μπροστά από το `sunlink`. Παρατηρήστε:

```
# chflags nosunlink file1
```

Για να δείτε τα flags ενός αρχείου, χρησιμοποιήστε την εντολή ls(1) με το πρόθεμα `-lo`:

```
# ls -lo file1
```

Στην έξοδο θα πρέπει να δείτε κάτι παρόμοιο με το ακόλουθο:

```
-rw-r--r--  1 trhodes  trhodes  sunlnk 0 Mar  1 05:54 file1
```

Μερικά flags μπορούν να προστεθούν ή να αφαιρεθούν μόνο από τον χρήστη `root`. Στις υπόλοιπες περιπτώσεις, ο ιδιοκτήτης του αρχείου μπορεί να θέσει αυτά τα flags. Προτείνουμε στους διαχειριστές να διαβάσουν τις σελίδες βοηθείας chflags(1) και chflags(2) για περισσότερες πληροφορίες.

5.3.3. Οι Άδειες setuid, setgid και sticky

Εκτός από τις άδειες που έχουμε συζητήσει ήδη, υπάρχουν τρεις ακόμα τις οποίες κάθε διαχειριστής πρέπει να γνωρίζει. Πρόκειται για τις άδειες `setuid`, `setgid` και `sticky`.

Οι παραπάνω είναι σημαντικές για κάποιες λειτουργίες στο UNIX®, καθώς παρέχουν λειτουργίες που δεν είναι φυσιολογικά διαθέσιμες στους κοινούς χρήστες. Για να τις κατανοήσετε, θα πρέπει πρώτα να καταλάβετε την διαφορά μεταξύ του πραγματικού αναγνωριστικού χρήστη (real user ID) και του ενεργού αναγνωριστικού χρήστη (effective user ID).

Το πραγματικό ID του χρήστη, είναι το UID στο οποίο ανήκει, ή με το οποίο ξεκινά, μια διεργασία. Το ενεργό UID, είναι το αναγνωριστικό χρήστη το οποίο εκτελεί την διεργασία. Για παράδειγμα, το βοηθητικό πρόγραμμα passwd(1) εκτελείται με το πραγματικό ID του χρήστη που αλλάζει τον κωδικό του. Ωστόσο, για να μπορεί να διαχειριστεί την βάση δεδομένων με τους κωδικούς του συστήματος, το πρόγραμμα αυτό χρησιμοποιεί ως ενεργό ID αυτό του χρήστη `root`. Με αυτό τον τρόπο, επιτρέπεται στους απλούς χρήστες να αλλάζουν τους κωδικούς τους χωρίς να παίρνουν το μήνυμα λάθους `Permission Denied` (απαγόρευση πρόσβασης).

Η επιλογή `nosuid` στην εντολή mount(8) θα προκαλέσει αποτυχία εκτέλεσης αυτών των εντολών, και μάλιστα χωρίς κάποιο μήνυμα λάθους. Με λίγα λόγια, η εκτέλεση τους θα αποτύχει, και ο χρήστης δεν θα ενημερωθεί για αυτό. Η επιλογή αυτή δεν είναι επίσης απόλυτα ασφαλής, καθώς (σύμφωνα με τη σελίδα manual mount(8)) υπάρχει τρόπος να παρακαμφθεί μέσω κάποιου ενδιάμεσου `nosuid` προγράμματος (wrapper).

Μπορείτε να καθορίσετε την άδεια setuid, τοποθετώντας τον αριθμό τέσσερα (4) μπροστά από το γενικό σετ των αδειών, όπως φαίνεται στο ακόλουθο παράδειγμα:

```
# chmod 4755 suidexample.sh
```

Οι άδειες στο αρχείο suidexample.sh θα φαίνονται τώρα όπως παρακάτω:

```
-rwsr-xr-x   1 trhodes  trhodes    63 Aug 29 06:36 suidexample.sh
```

Παρατηρήστε στο παράδειγμα, ότι το `s` είναι πλέον μέλος του συνόλου αδειών που έχουν καθοριστεί για τον ιδιοκτήτη του αρχείου, και έχει αντικαταστήσει την αντίστοιχη άδεια εκτέλεσης. Με τον τρόπο αυτό λειτουργούν προγράμματα που χρειάζονται αυξημένα δικαιώματα, όπως για παράδειγμα η εντολή `passwd`.

Για να παρατηρήσετε αυτή τη λειτουργία την ώρα που συμβαίνει, ανοίξτε δύο τερματικά. Στο πρώτο, ξεκινήστε την εντολή `passwd` ως κανονικός χρήστης. Καθώς η εντολή εκτελείται και περιμένει για την εισαγωγή του νέου κωδικού, ελέγξτε τον πίνακα διεργασιών και αναζητήστε τις πληροφορίες του χρήστη που εκτελεί την εντολή `passwd`.

Στο τερματικό A:

```
Changing local password for trhodes
Old Password:
```

Στο τερματικό B:

```
# ps aux | grep passwd
```

```
trhodes  5232  0.0  0.2  3420  1608   0  R+    2:10AM   0:00.00 grep passwd
root     5211  0.0  0.2  3620  1724   2  I+    2:09AM   0:00.01 passwd
```

Όπως είπαμε παραπάνω, η εντολή `passwd` εκτελείται από ένα κανονικό χρήστη, αλλά χρησιμοποιεί το ενεργό UID του χρήστη `root`.

Η άδεια `setgid` εκτελεί την ίδια λειτουργία όπως και η `setuid`, αλλά επιδρά στις άδειες της ομάδας (group). Όταν εκτελέσετε μια τέτοια εφαρμογή ή βοηθητικό πρόγραμμα, θα χρησιμοποιεί τις άδειες της ομάδας στην οποία ανήκει το αρχείο, και όχι του χρήστη που την ξεκίνησε.

Για να θέσετε την άδεια `setgid` σε ένα αρχείο, θα πρέπει να τοποθετήσετε τον αριθμό δύο (2) μπροστά από το σύνολο αδειών, στην εντολή `chmod`. Δείτε το παρακάτω παράδειγμα:

```
# chmod 2755 sgidexample.sh
```

Όπως και πριν, θα παρατηρήσετε τη νέα άδεια `s`, αλλά αυτή τη φορά στο σετ των αδειών της ομάδας:

```
-rwxr-sr-x   1 trhodes  trhodes    44 Aug 31 01:49 sgidexample.sh
```

Στα παραδείγματα μας, αν και το αρχείο είναι ένα εκτελέσιμο script για κέλυφος, δεν θα εκτελεστεί με διαφορετικό ενεργό ID (EUID). Αυτό συμβαίνει γιατί σε αυτά τα scripts δεν επιτρέπεται η πρόσβαση στις κλήσεις setuid(2) του συστήματος.

Οι δύο πρώτες ειδικές άδειες που αναφέραμε, οι `setuid` και `setgid`, ενδεχομένως να μειώσουν την ασφάλεια του συστήματος, αφού επιτρέπουν σε προγράμματα να εκτελούνται με αυξημένα δικαιώματα. Υπάρχει ωστόσο μια τρίτη ειδική άδεια, η οποία μπορεί να αυξήσει την ασφάλεια του συστήματος: το `sticky bit`.

Όταν θέσετε το `sticky bit` σε ένα κατάλογο, επιτρέπεται η διαγραφή ενός αρχείου μόνο από τον ιδιοκτήτη του. Η άδεια αυτή είναι χρήσιμη για να αποφεύγεται η διαγραφή ενός αρχείου από

κοινόχρηστους καταλόγους, όπως για παράδειγμα ο /tmp, από κάποιο χρήστη που δεν είναι ο ιδιοκτήτης του. Για να θέσετε αυτή την άδεια, τοποθετήστε τον αριθμό ένα (1) στην αρχή του σετ αδειών:

```
# chmod 1777 /tmp
```

Μπορείτε τώρα να δείτε το αποτέλεσμα, χρησιμοποιώντας την εντολή `ls`:

```
# ls -al / | grep tmp
```

```
drwxrwxrwt  10 root  wheel         512 Aug 31 01:49 tmp
```

Η άδεια `sticky bit` φαίνεται ως `t` στο τέλος του συνόλου των αδειών.

5.4. Δομή Καταλόγου

Η ιεραρχική δομή του FreeBSD είναι ένα βασικό στοιχείο που πρέπει να γνωρίζετε αν θέλετε να έχετε μια ολοκληρωμένη εικόνα του συστήματος. Η πιο σημαντική έννοια είναι αυτή του ριζικού (root) καταλόγου, "/". Αυτός ο κατάλογος προσαρτάται (mount) πρώτος κατά την εκκίνηση και περιέχει το βασικό σύστημα ικανό να ετοιμάσει το Λ.Σ. για λειτουργία multi-user. Ο root κατάλογος περιέχει επίσης σημεία προσάρτησης για άλλα συστήματα αρχείων που προσαρτώνται κατά την μετάβαση σε κατάσταση λειτουργίας multi-user.

Σημείο προσάρτησης (mount point) είναι ένας κατάλογος στον οποίο μπορούν να αναπτυχθούν πρόσθετα συστήματα αρχείων σε ένα γονικό σύστημα αρχείων (συνήθως στο root σύστημα αρχείων). Αυτό περιγράφεται αναλυτικά στην ενότητα Οργάνωση Δίσκου. Στα στάνταρντ σημεία προσάρτησης περιλαμβάνονται: οι /usr, /var, /tmp, /mnt, και /cdrom. Αυτοί οι κατάλογοι συνήθως είναι καταχωρημένοι στο αρχείο /etc/fstab. Το /etc/fstab είναι ένας πίνακας αντιστοιχίας διαφόρων συστημάτων αρχείων και σημείων προσάρτησης για αναφορά στο σύστημα. Τα περισσότερα συστήματα που αναφέρονται στο /etc/fstab προσαρτώνται αυτόματα κατά την εκκίνηση του συστήματος από το script rc(8) εκτός αν περιέχεται η επιλογή `noauto`. Λεπτομέρειες μπορείτε να βρείτε στο Το Αρχείο fstab.

Μια πλήρη περιγραφή της ιεραρχίας του συστήματος αρχείων είναι διαθέσιμη στο hier(7). Ακολουθεί μια σύντομη ανασκόπηση με τους πιο συνήθεις καταλόγους.

Κατάλογος	Περιγραφή
/	Ριζικός (root) κατάλογος του συστήματος αρχείων.
/bin/	Χρήσιμα εργαλεία για περιβάλλον ενός ή πολλαπλών χρηστών.
/boot/	Προγράμματα και αρχεία ρυθμίσεων που χρησιμοποιούνται κατά την εκκίνηση του λειτουργικού συστήματος.

Κατάλογος	Περιγραφή
/boot/defaults/	Προκαθορισμένα αρχεία ρυθμίσεων εκκίνησης, δείτε loader.conf(5).
/dev/	Αρχεία συσκευών, δείτε intro(4).
/etc/	Αρχεία ρυθμίσεων συστήματος και σενάρια εκκίνησης.
/etc/defaults/	Προκαθορισμένα αρχεία ρυθμίσεων συστήματος, δείτε την rc(8).
/etc/mail/	Αρχεία ρυθμίσεων για πράκτορες μεταφοράς ηλεκτρ. ταχυδρομείου (MTA) όπως το sendmail(8).
/etc/namedb/	Αρχεία ρυθμίσεων `named`, δείτε named(8).
/etc/periodic/	Σενάρια λειτουργιών που τρέχουν σε ημερήσια, εβδομαδιαία, και μηνιαία βάση, cron(8); δείτε periodic(8).
/etc/ppp/	Αρχεία ρυθμίσεων `ppp`, δείτε τις ppp(8).
/mnt/	Κενός κατάλογος που συνήθως χρησιμοποιείται από τους διαχειριστές συστημάτων ως προσωρινό σημείο προσάρτησης.
/proc/	Σύστημα αρχείων διεργασιών, δείτε τις procfs(5), mount_procfs(8).
/rescue/	Προγράμματα με στατική σύνδεση (static link) για ασφαλή επαναφορά συστήματος, δείτε την rescue(8).
/root/	Προσωπικός κατάλογος του χρήστη `root`.
/sbin/	Προγράμματα συστήματος και χρήσιμα εργαλεία διαχείρισης για περιβάλλον ενός ή πολλαπλών χρηστών.
/tmp/	Προσωρινά αρχεία. Τα περιεχόμενα του /tmp συνήθως δεν διατηρούνται μετά από επανεκκίνηση του συστήματος. Στο /tmp συνήθως προσαρτάται ένα σύστημα αρχείων μνήμης. Αυτό μπορεί να επιτευχθεί αυτομάτως χρησιμοποιώντας τις σχετικές μεταβλητές tmpmfs του rc.conf(5) (ή με μια καταχώρηση στον /etc/fstab, δείτε την mdmfs(8)).
/usr/	Περιέχονται σχεδόν όλα τα βοηθητικά προγράμματα και οι εφαρμογές χρηστών.
/usr/bin/	Κοινόχρηστα βοηθητικά προγράμματα, εργαλεία προγραμματισμού, και εφαρμογές.
/usr/include/	Στάνταρ αρχεία συμπερίληψης C (include files).

Κατάλογος	Περιγραφή
/usr/lib/	Αρχεία βιβλιοθηκών.
/usr/libdata/	Διάφορα αρχεία δεδομένων βοηθητικών προγραμμάτων.
/usr/libexec/	Δαίμονες συστήματος & βοηθητικά προγράμματα συστήματος (εκτελούνται από άλλα προγράμματα).
/usr/local/	Τοπικά εκτελέσιμα, βιβλιοθήκες, κτλ. Επίσης είναι και ο προκαθορισμένος προορισμός για προγράμματα που εγκαθίστανται από τα ports του FreeBSD. Μέσα στον /usr/local, χρησιμοποιείται γενικά η διάταξη του /usr που περιγράφεται στο hier(7). Εξαιρούνται οι κατάλογοι σελίδων βοηθείας man, που βρίσκεται άμεσα κάτω από τον /usr/local και όχι κάτω από τον /usr/local/share, καθώς και η τεκμηρίωση κάθε port που βρίσκεται στον share/doc/port.
/usr/obj/	Δέντρο προορισμού που εξαρτάται από την αρχιτεκτονική του μηχανήματος και παράγεται μεταγλωττίζοντας το δέντρο /usr/src.
/usr/ports/	Η Συλλογή Ports του FreeBSD (προαιρετικό).
/usr/sbin/	Δαίμονες συστήματος & βοηθητικά προγράμματα συστήματος (εκτελούνται από χρήστες).
/usr/shared/	Αρχεία ανεξάρτητα από την Αρχιτεκτονική του μηχανήματος.
/usr/src/	Αρχεία BSD και/ή τοπικά αρχεία πηγαίου κώδικα.
/usr/X11R6/	Εκτελέσιμα, βιβλιοθήκες, κτλ. για την διανομή X11R6 (προαιρετικό).
/var/	Αρχεία αναφοράς (log) διαφόρων χρήσεων, temporary, transient, και spool. Μερικές φορές προσαρτάται στον /var ένα σύστημα αρχείων μνήμης. Αυτό μπορεί να επιτευχθεί αυτόματα χρησιμοποιώντας τις σχετικές μεταβλητές varmfs του rc.conf(5) (ή με μία καταχώρηση στο /etc/fstab, δείτε τις mdmfs(8)).
/var/log/	Διάφορα αρχεία συμβάντων του συστήματος.
/var/mail/	Αρχεία γραμματοκιβωτίου (mailbox) χρηστών.
/var/spool/	Διάφοροι κατάλογοι παροχέτευσης (spool) εκτυπωτών και ηλεκτρονικής αλληλογραφίας του συστήματος.

Κατάλογος	Περιγραφή
/var/tmp/	Προσωρινά (temporary) αρχεία. Τα αρχεία αυτά συνήθως διατηρούνται κατά την διάρκεια επανεκκίνησης του συστήματος, εκτός αν ο /var είναι ένα σύστημα αρχείων μνήμης.
/var/yp/	Απεικονίσεις (maps) NIS.

5.5. Οργάνωση Δίσκου

Η μικρότερη μονάδα οργάνωσης που χρησιμοποιεί το FreeBSD για να βρει αρχεία είναι το όνομα αρχείου. Τα ονόματα αρχείων είναι ευαίσθητα στα κεφαλαία- μικρά, το οποίο σημαίνει ότι το readme.txt και το README.TXT είναι δύο διαφορετικά αρχεία. Το FreeBSD δεν χρησιμοποιεί την επέκταση .txt αρχείου για να προσδιορίσει αν ένα αρχείο είναι πρόγραμμα, ή έγγραφο, ή άλλος τύπος δεδομένων.

Τα αρχεία αποθηκεύονται σε καταλόγους. Ένας κατάλογος μπορεί να μην περιέχει αρχεία, ή μπορεί να περιέχει εκατοντάδες αρχεία. Ένας κατάλογος μπορεί επίσης να περιέχει άλλους καταλόγους, επιτρέποντας σας να κατασκευάσετε μια ιεραρχική δομή καταλόγων όπου κατάλογοι εσωκλείουν άλλους καταλόγους. Αυτό μας επιτρέπει να οργανώσουμε τα δεδομένα μας πολύ ευκολότερα.

Η αναφορά σε αρχεία και καταλόγους γίνεται δίνοντας το όνομα αρχείου ή το όνομα καταλόγου, ακολουθεί μία αριστερόστροφη κάθετος, / και έπειτα οποιοδήποτε άλλο κατάλληλο όνομα καταλόγου. Εάν έχετε τον κατάλογο foo, ο οποίος περιέχει τον κατάλογο bar, ο οποίος περιέχει το αρχείο readme.txt, τότε το ολοκληρωμένο όνομα, *διαδρομή (path)* στο αρχείο είναι foo/bar/readme.txt.

Κατάλογοι και αρχεία αποθηκεύονται σε ένα σύστημα αρχείων. Κάθε σύστημα αρχείων περιέχει ένα κατάλογο στο ανώτερο επίπεδο, που ονομάζεται *root (ριζικός) κατάλογος* για το συγκεκριμένο σύστημα αρχείων. Ο root κατάλογος μπορεί να περιέχει άλλους καταλόγους.

Αυτό πιθανώς είναι παρόμοιο με οποιοδήποτε άλλο λειτουργικό σύστημα έχετε χρησιμοποιήσει. Ωστόσο υπάρχουν μερικές διαφορές. Για παράδειγμα, το MS-DOS® χρησιμοποιεί \ για να διαχωρίζει ονόματα καταλόγων και αρχείων, ενώ το Mac OS® χρησιμοποιεί :.

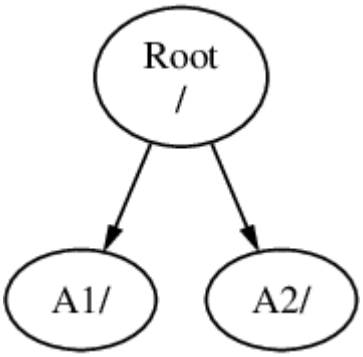
Το FreeBSD δεν χρησιμοποιεί γράμματα οδηγών ή ονόματα οδηγών στη διαδρομή. Επομένως δεν θα πρέπει να γράφετε c:/foo/bar/readme.txt στο FreeBSD.

Αντιθέτως, ένα σύστημα αρχείων καθορίζεται ως root σύστημα αρχείων. Ο ριζικός κατάλογος του root συστήματος αρχείων αναφέρεται ως /. Κάθε άλλο σύστημα αρχείου *προσαρτάται* κάτω από το root σύστημα αρχείων Δεν έχει σημασία πόσους δίσκους έχετε στο FreeBSD σύστημα σας, κάθε κατάλογος εμφανίζεται να είναι μέρος του ίδιου δίσκου.

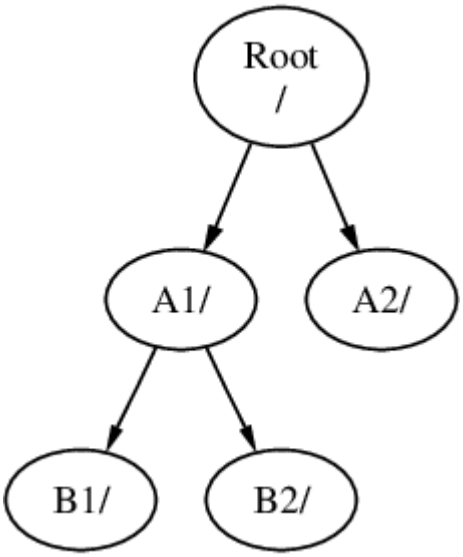
Ας υποθέσουμε πως έχετε τρία συστήματα αρχείων, τα ονομάζουμε A, B και C. Κάθε σύστημα αρχείου έχει έναν ριζικό κατάλογο, ο οποίος περιέχει δύο άλλους καταλόγους, που τους ονομάζουμε A1, A2 (και παρομοίως B1, B2 και C1, C2).

Ας θεωρήσουμε ότι το A είναι το root σύστημα αρχείων. Αν χρησιμοποιήσετε την εντολή ls για να δείτε τα περιεχόμενα αυτού του καταλόγου, θα δείτε δύο υποκαταλόγους, A1 και A2. Το δέντρο του

καταλόγου μοιάζει σαν αυτό:

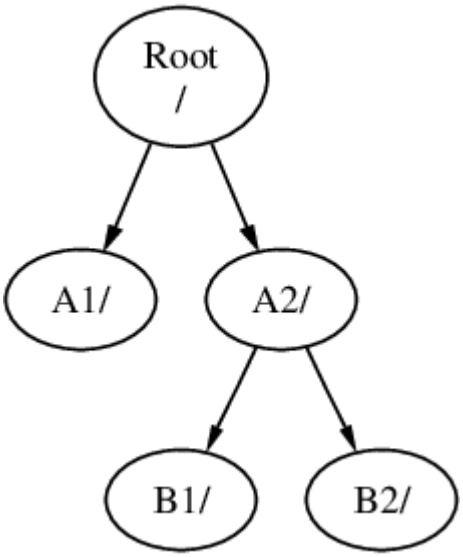


Κάθε σύστημα αρχείων πρέπει να προσαρτάται σε ένα κατάλογο διαφορετικού συστήματος αρχείων. Ας υποθέσουμε πως θέλετε να προσαρτήσετε το σύστημα αρχείου B στον κατάλογο A1. Ο ριζικός κατάλογος του B αντικαθιστά τον A1, και οι κατάλογοι του B εμφανίζονται αναλόγως:



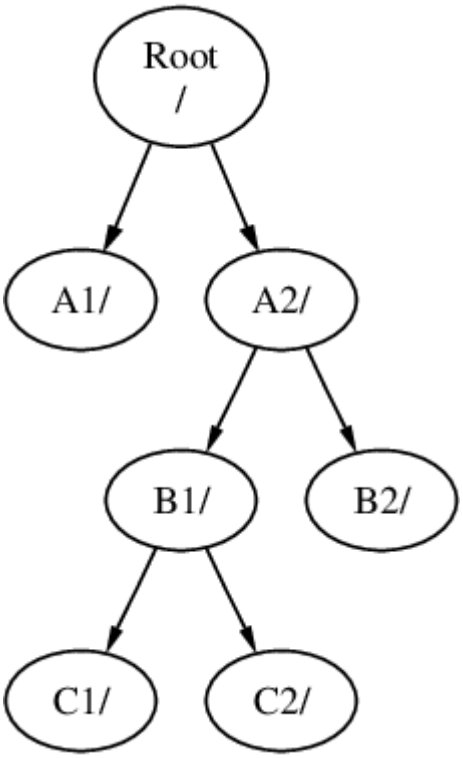
Όλα τα αρχεία που περιέχονται στους καταλόγους B1 και B2 τα βρίσκουμε με τη διαδρομή /A1/B1 ή με /A1/B2 αντίστοιχα. Όλα τα αρχεία που βρίσκονταν στο /A1 είναι προσωρινά κρυμμένα. Θα επανεμφανιστούν όταν ο B θα *αποπροσαρτηθεί* από τον A.

Αν ο B είχε προσαρτηθεί στον A2 τότε το διάγραμμα θα έδειχνε κάπως έτσι:

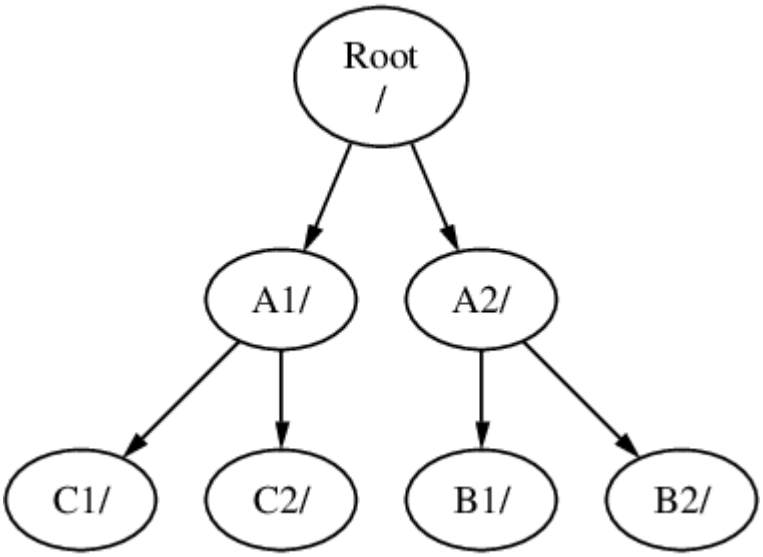


και οι διαδρομές θα ήταν /A2/B1 και /A2/B2 αντίστοιχα.

Τα συστήματα αρχείων μπορούν να προσαρτώνται στην κορυφή άλλων συστημάτων. Συνεχίζοντας το τελευταίο παράδειγμα, το σύστημα αρχείου `C` θα μπορούσε να προσαρτηθεί στην κορυφή του καταλόγου `B1` στο σύστημα αρχείου `B`, οδηγώντας σε αυτήν την κατανομή:



Ή ακόμη το `C` θα μπορούσε να προσαρτηθεί άμεσα στο σύστημα αρχείου `A`, κάτω από τον κατάλογο `A1`:



Αν γνωρίζετε το σύστημα MS-DOS®, είναι παρόμοιο, αλλά όχι ακριβώς το ίδιο, με την εντολή `join`.

Αυτό συνήθως δεν είναι κάτι που πρέπει να γνωρίζετε άμεσα. Τυπικά, εσείς δημιουργείτε συστήματα αρχείων όταν εγκαθιστάτε το FreeBSD και αποφασίζετε το σημείο προσάρτησης αυτών, και έπειτα δεν χρειάζεται να τα αλλάξετε εκτός αν πρόκειται να προσθέσετε ένα καινούργιο δίσκο.

Είναι απόλυτα δυνατόν να έχετε ένα μεγάλο root σύστημα αρχείων, και να μην χρειάζεται να δημιουργήσετε άλλα. Με αυτή την τακτική υπάρχουν μερικά μειονεκτήματα και ένα πλεονέκτημα.

Προτερήματα Πολλαπλών Συστημάτων Αρχείων

- Διαφορετικά συστήματα αρχείων μπορούν να έχουν διαφορετικές *επιλογές προσάρτησης*. Για παράδειγμα, με προσεκτικό σχεδιασμό, το root σύστημα αρχείων μπορεί να προσαρτηθεί μόνο για ανάγνωση, ώστε να είναι αδύνατη η διαγραφή ή η μετατροπή κάποιου σημαντικού αρχείου. Διαχωρίζοντας συστήματα αρχείων με δυνατότητα εγγραφής από τον χρήστη, όπως ο /home, επιτρέπει επίσης την προσάρτηση τους ως *nosuid*. Αυτή η επιλογή περιορίζει την χρήση εκτελέσιμων που είναι αποθηκευμένα στο σύστημα αρχείων, με ενεργοποιημένα τα bits *suid* /*guid*, βελτιώνοντας πιθανώς την ασφάλεια.
- Ανάλογα με το πως θα χρησιμοποιηθεί το σύστημα αρχείων, το FreeBSD ρυθμίζει με τον καλύτερο τρόπο την διάταξη των αρχείων στο σύστημα. Επομένως ένα σύστημα που περιέχει πολλά μικρά αρχεία που μεταβάλλονται συχνά, θα έχει διαφορετική διάταξη από ένα άλλο που περιέχει λιγότερα σε αριθμό, αλλά πιο ογκώδη αρχεία. Εάν έχετε ένα μοναδικό σύστημα αρχείων, τότε χάνετε αυτή τη δυνατότητα.
- Τα συστήματα αρχείων του FreeBSD είναι πολύ ισχυρά. Ωστόσο, μια αδυναμία σε κάποιο σημαντικό σημείο μπορεί ακόμη να οδηγήσει σε κατάρρευση της δομής του συστήματος αρχείων. Ο διαχωρισμός των δεδομένων σας σε πολλαπλά συστήματα αρχείων κάνει πιο εύκολη μια πιθανή επαναφορά από backup, όταν αυτό είναι αναγκαίο.

Προτερήματα ενός Μονοκόμματου Συστήματος Αρχείου

- Τα συστήματα αρχείων είναι συγκεκριμένου σταθερού μεγέθους. Αν δημιουργήσετε ένα σύστημα αρχείων κατά την εγκατάσταση του FreeBSD και του δώσετε ένα ορισμένο μέγεθος, μπορεί αργότερα να ανακαλύψετε πως χρειάζεστε να φτιάξετε μια μεγαλύτερη κατάτμηση. Αυτό δεν είναι εύκολα πραγματοποιήσιμο δίχως backup, αναδημιουργία του συστήματος αρχείου με

το νέο μέγεθος, και επαναφορά των αποθηκευμένων δεδομένων.

Στο FreeBSD περιέχεται η εντολή growfs(8), η οποία επιτρέπει να αυξήσουμε το μέγεθος ενός συστήματος αρχείων κατά τη λειτουργία του, αφαιρώντας αυτόν τον περιορισμό.

Τα συστήματα αρχείων περιέχονται σε κατατμήσεις (partitions). Αυτό δεν έχει την ίδια έννοια με την κοινή χρήση του όρου κατάτμηση (όπως για παράδειγμα, η κατάτμηση του MS-DOS®), λόγω της κληρονομιάς που φέρει το FreeBSD από το UNIX®. Κάθε κατάτμηση αναγνωρίζεται από ένα λατινικό χαρακτήρα ξεκινώντας από a έως το h. Κάθε κατάτμηση μπορεί να περιέχει μόνο ένα σύστημα αρχείων, το οποίο σημαίνει πως η αναφορά στα συστήματα αρχείων γίνεται είτε από το τυπικό σημείο προσάρτησης στην ιεραρχία του συστήματος αρχείων, είτε από το λατινικό χαρακτήρα της κατάτμησης.

Επίσης το FreeBSD χρησιμοποιεί μέρος από το δίσκο για *χώρο swap*. Ο χώρος Swap παρέχει στο FreeBSD *εικονική μνήμη (virtual memory)*. Αυτό επιτρέπει στον υπολογιστή σας να συμπεριφέρεται σαν να είχε πολύ περισσότερη μνήμη από όσο πραγματικά έχει. Όταν το FreeBSD δεν έχει διαθέσιμη μνήμη μεταφέρει μερικά από τα δεδομένα που δεν χρησιμοποιούνται, την προκειμένη στιγμή, στον χώρο swap, και όταν τα χρειαστεί τα επαναφέρει (ενώ μεταφέρει κάποια άλλα δεδομένα στον χώρο swap).

Υπάρχουν κάποιες συμβάσεις σχετικά με τις κατατμήσεις

Κατάτμηση	**Σύμβαση**
a	Συνήθως περιλαμβάνει το root σύστημα αρχείων
b	Συνήθως περιλαμβάνει τον χώρο swap
c	Συνήθως ιδίου μεγέθους με την περιλαμβανόμενη φέτα (slice). Αυτό επιτρέπει σε βοηθητικά προγράμματα που πρέπει να δουλέψουν σε ολόκληρο το κομμάτι (για παράδειγμα, ένας ανιχνευτής κατεστραμμένων μπλοκ) να λειτουργούν στην c κατάτμηση. Κανονικά δεν θα πρέπει να δημιουργείτε σύστημα αρχείων σε αυτή την κατάτμηση.
d	Η κατάτμηση d είχε στο παρελθόν μια ειδική αντιστοιχία, κάτι που δεν ισχύει πλέον σήμερα, επομένως η d μπορεί να χρησιμοποιείται σαν μια κανονική κατάτμηση.

Κάθε κατάτμηση που περιέχει ένα σύστημα αρχείων αποθηκεύεται στο FreeBSD σε μια τοποθεσία που ονομάζεται *φέτα (slice)*. Η φέτα είναι ένας όρος του FreeBSD για αυτό που κοινώς αποκαλείται κατάτμηση, και αυτό επίσης οφείλεται στην καταγωγή του FreeBSD από το UNIX®. Οι φέτες αριθμούνται αρχίζοντας από το 1 έως το 4.

Ο αριθμός της φέτας ακολουθεί το όνομα συσκευής μετά το πρόθεμα s ξεκινώντας από το 1. Επομένως, "da0*s1*" είναι η πρώτη φέτα του πρώτου οδηγού SCSI. Μπορούν να υπάρχουν μέχρι τέσσερις φέτες σε κάθε δίσκο, αλλά μπορείτε να δημιουργήσετε λογικές φέτες μέσα σε κατάλληλου

τύπου φυσικές φέτες. Σε αυτές τις εκτεταμένες φέτες η αρίθμηση ξεκινάει από το 5, επομένως "ad0*s5*" είναι η πρώτη εκτεταμένη φέτα στον πρώτο δίσκο IDE. Αυτές οι συσκευές χρησιμοποιούνται από συστήματα αρχείων που πρέπει να καταλαμβάνουν μια ολόκληρη φέτα.

Οι φέτες, οι "επικίνδυνα αφοσιωμένοι (dangerously dedicated) " φυσικοί οδηγοί καθώς και άλλοι οδηγοί, περιέχουν *κατατμήσεις*, οι οποίες παρουσιάζονται με λατινικούς χαρακτήρες από το a έως το h. Αυτός ο χαρακτήρας αναφέρεται στο όνομα συσκευής, επομένως "da0*a*" είναι η a κατάτμηση στον πρώτο οδηγό da, ο οποίος είναι "επικίνδυνα αφοσιωμένος". Η "ad1s3*e*" είναι η πέμπτη κατάτμηση στην τρίτη φέτα του δεύτερου οδηγού δίσκου IDE.

Ολοκληρώνοντας, κάθε δίσκος στο σύστημα είναι μονόδρομα ορισμένος. Κάθε όνομα δίσκου ξεκινά με ένα κωδικό που υποδεικνύει τον τύπο του δίσκου, και ένα νούμερο που υποδηλώνει ποιος δίσκος είναι. Αντίθετα με τις φέτες, οι δίσκοι αριθμούνται ξεκινώντας από το 0. Οι πιο συνήθεις κωδικοί που θα συναντήσετε αναφέρονται στην Κωδικοί Συσκευών Δίσκων.

Όταν γίνεται αναφορά σε μια κατάτμηση, το FreeBSD ζητά να δηλωθεί επιπλέον η ονομασία της φέτας και του δίσκου που περιέχει την κατάτμηση, ενώ στην περίπτωση που αναφέρεστε σε μια φέτα θα πρέπει να δηλώνετε το όνομα του δίσκου. Επομένως, όταν αναφέρεστε σε μια κατάτμηση χρειάζεται να δηλώνετε το όνομα του δίσκου, s, τον αριθμό της φέτας, και τον χαρακτήρα της κατάτμησης. Παραδείγματα μπορείτε να βρείτε στην Υποδείγματα Ονομάτων Δίσκου, Φέτας, Κατάτμησης.

Η Εννοιολογικό Μοντέλο ενός Δίσκου παρουσιάζει ένα εννοιολογικό μοντέλο για τη δομή του δίσκου που θα σας βοηθήσει να καταλάβετε καλύτερα κάποια πράγματα.

Για να εγκαταστήσετε το FreeBSD πρέπει πρώτα να ρυθμίσετε τις φέτες του δίσκου, να δημιουργήσετε τις κατατμήσεις μέσα στις φέτες που θα χρησιμοποιήσετε για το FreeBSD, έπειτα να δημιουργήσετε ένα σύστημα αρχείων (ή χώρο swap) σε κάθε κατάτμηση, και τέλος να αποφασίσετε σε ποιο σημείο θα προσαρτηθεί το σύστημα αρχείων.

Πίνακας 2. Κωδικοί Συσκευών Δίσκων

Κώδικας	Σημαίνει
ad	Δίσκος ATAPI (IDE)
da	Δίσκος SCSI άμεσης πρόσβασης
acd	ATAPI (IDE) CDROM
cd	SCSI CDROM
fd	Μονάδα Δισκέτας (Floppy)

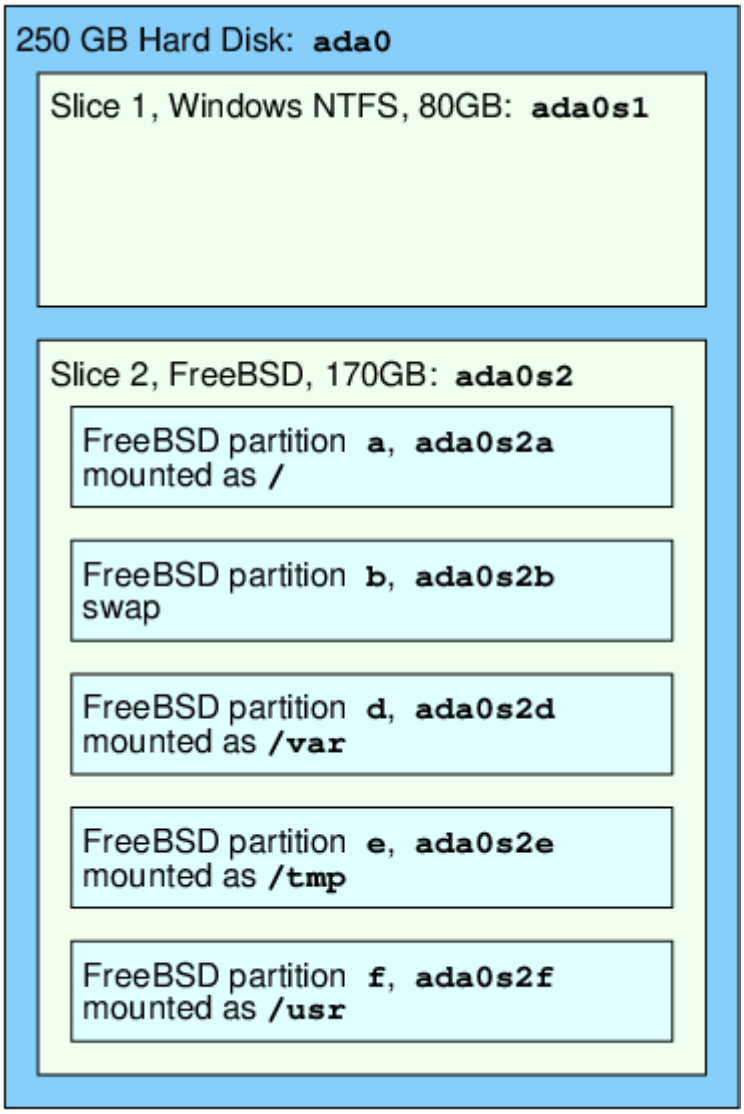
Παράδειγμα 4. Υποδείγματα Ονομάτων Δίσκου, Φέτας, Κατάτμησης

Ονομασία	Σημαίνει
`ad0s1a`	Η πρώτη κατάτμηση (`a`) στην πρώτη φέτα (`s1`) του πρώτου δίσκου IDE (`ad0`).
`da1s2e`	Η πέμπτη κατάτμηση (`e`) στην δεύτερη φέτα (`s2`) του δεύτερου δίσκου SCSI (`da1`).

Παράδειγμα 5. Εννοιολογικό Μοντέλο ενός Δίσκου

Το διάγραμμα παρουσιάζει μια εικόνα του πρώτου δίσκου IDE που είναι προσαρτημένος στο σύστημα. Ας υποθέσουμε πως ο δίσκος έχει μέγεθος 4 GB, και περιέχει δύο φέτες των 2 GB (κατατμήσεις MS-DOS®). Η πρώτη φέτα περιέχει ένα δίσκο MS-DOS®, C:, και η δεύτερη φέτα μία εγκατάσταση FreeBSD. Σε αυτό το παράδειγμα, η εγκατάσταση FreeBSD έχει τρεις κατατμήσεις δεδομένων και μία κατάτμηση swap.

Καθεμία από τις τρεις κατατμήσεις θα περιέχει ένα σύστημα αρχείων. Η κατάτμηση `a` θα χρησιμοποιηθεί για το root σύστημα αρχείων, η `e` για τη δομή κατάλογου /var, και η `f` για τη δομή καταλόγου /usr.



5.6. Προσάρτηση και Αποπροσάρτηση Συστημάτων Αρχείων

Ένα σύστημα αρχείων αναπαριστάται καλύτερα σε μορφή δέντρου, με τις ρίζες του στο /. Οι κατάλογοι /dev, /usr, και άλλοι είναι κλαδιά του καταλόγου root, και μπορεί να έχουν με τη σειρά τους, τα δικά τους κλαδιά, όπως τον /usr/local, και ούτω καθεξής.

Υπάρχουν διάφοροι λόγοι για τους οποίους θα έπρεπε να τοποθετήσουμε κάποιους από αυτούς τους καταλόγους σε διαφορετικά συστήματα αρχείων. Ο κατάλογος /var περιέχει τους καταλόγους log/, spool/, και διάφορους άλλους τύπους προσωρινών αρχείων, και για το λόγο αυτό μπορεί να γεμίσει. Δεν θα ήταν καλή ιδέα να γεμίσει το root σύστημα αρχείων, επομένως ο διαχωρισμός του /var από τον / είναι συχνά επιθυμητός.

Ένας άλλος συνηθισμένος λόγος να έχουμε διάφορους καταλόγους σε διαφορετικά συστήματα αρχείων είναι όταν πρόκειται να φιλοξενηθούν σε διαφορετικούς φυσικούς δίσκους, ή είναι ξεχωριστοί εικονικοί δίσκοι, όπως συμβαίνει με το Δικτυακό Σύστημα Αρχείων (Network File System), και τους οδηγούς CDROM.

5.6.1. Το Αρχείο fstab

Κατά τη διεργασία εκκίνησης, τα συστήματα αρχείων που αναφέρονται στο /etc/fstab προσαρτώνται αυτόματα (εκτός αν αναφέρονται με την επιλογή `noauto`).

Το αρχείο /etc/fstab περιέχει μια σειρά από γραμμές με διάταξη όπως η ακόλουθη:

```
device       /mount-point fstype     options      dumpfreq     passno
```

`device`

Όνομα συσκευής (η οποία θα πρέπει να υπάρχει), όπως εξηγείται στην Device Names.

`mount-point`

Κατάλογος (θα πρέπει να υπάρχει) στον οποίο προσαρτάται το σύστημα αρχείων.

`fstype`

Ο τύπος του συστήματος αρχείων που θα δοθεί στην mount(8). Το προκαθορισμένο σύστημα αρχείων του FreeBSD είναι το `ufs`.

`options`

Το `rw` για συστήματα αρχείων ανάγνωσης- εγγραφής (read- write), ή `ro` για συστήματα αρχείων μόνο ανάγνωσης (read-only), συμπληρωμένο με όποια άλλη επιλογή μπορεί να χρειάζεστε. Μία συνήθης επιλογή είναι η `noauto` για συστήματα αρχείων που δεν προσαρτώνται αυτόματα κατά τις διεργασίες εκκίνησης του συστήματος. Άλλες επιλογές αναφέρονται στην σελίδα βοήθειας mount(8).

`dumpfreq`

Αυτό το πεδίο χρησιμοποιείται από το dump(8) για να ορίσει ποια συστήματα αρχείων χρειάζονται dumping. Αν το πεδίο απουσιάζει, τότε η προκαθορισμένη τιμή του είναι μηδέν.

`passno`

Αυτό ορίζει την σειρά με την οποία θα ελέγχονται τα συστήματα αρχείων. Συστήματα αρχείων που δεν επιθυμούμε να ελεγχθούν θα πρέπει να έχουν στο πεδίο `passno` τιμή μηδέν. Το root σύστημα αρχείων (το οποίο πρέπει να ελεγχθεί πριν από όλα τα άλλα) θα έχει στο πεδίο `passno` την τιμή ένα και όλα τα άλλα συστήματα αρχείων θα έχουν στο πεδίο `passno` τιμές μεγαλύτερες από ένα. Αν περισσότερα από ένα συστήματα αρχείων έχουν την ίδια τιμή `passno` τότε το fsck(8)

θα επιχειρήσει να ελέγξει παράλληλα τα συστήματα αρχείων, αν αυτό είναι εφικτό.

Συμβουλευτείτε την σελίδα βοηθείας fstab(5) για περισσότερες πληροφορίες για την μορφή του αρχείου /etc/fstab και για τις επιλογές που μπορεί να περιέχει.

5.6.2. Η Εντολή `mount`

Η εντολή mount(8) είναι αυτό ακριβώς που χρειάζεστε για την προσάρτηση συστημάτων αρχείων.

Η βασική μορφή της είναι:

```
# mount device mountpoint
```

Υπάρχει πληθώρα επιλογών, όπως αναφέρεται στην σελίδα βοηθείας mount(8), αλλά οι πιο συνήθεις είναι:

Επιλογές εντολής mount

`-a`

Προσάρτηση όλων των συστημάτων αρχείων που αναφέρονται στο /etc/fstab, εκτός αυτών που φέρουν την επιλογή "noauto", εξαιρούνται μέσω της επιλογής `-t`, ή αυτών που ήδη έχουν προσαρτηθεί.

`-d`

Κάνει τα πάντα εκτός από την πραγματική προσάρτηση του συστήματος. Αυτή η επιλογή είναι χρήσιμη σε συνεργασία με το πρόθεμα `-v` για να προσδιοριστεί τι ακριβώς προσπαθεί να κάνει η mount(8) την συγκεκριμένη στιγμή.

`-f`

Αναγκάζει την προσάρτηση ενός μη-καθαρού συστήματος αρχείων (επικίνδυνο), ή εξαναγκάζει την ανάκληση πρόσβασης εγγραφής όταν υποβιβάζεται η προσάρτηση ενός συστήματος αρχείων ανάγνωσης-εγγραφής (read-write) σε μόνο-ανάγνωσης.

`-r`

Προσαρτά το σύστημα αρχείων σε κατάσταση μόνο-ανάγνωσης. Είναι ακριβώς το ίδιο με τη χρήση του προθέματος `ro` με την επιλογή `-o`.

`-t` ***fstype***

Προσαρτά το υπάρχον σύστημα αρχείων, χρησιμοποιώντας τον τύπο συστήματος αρχείων που δίνεται, ή προσαρτά μόνο συστήματα αρχείων του συγκεκριμένου τύπου, εάν δοθεί μαζί με την επιλογή `-a`.

Το "ufs" είναι ο προεπιλεγμένος τύπος συστήματος αρχείων.

`-u`

Ανανεώνει τις επιλογές προσάρτησης στο σύστημα αρχείων.

`-v`

Συμπεριλαμβάνει αναλυτική αναφορά.

`-w`

Προσαρτά το σύστημα αρχείων για ανάγνωση-εγγραφή (read-write).

Η επιλογή `-o` δέχεται μία σειρά από επιλογές χωρισμένες με κόμμα, περιλαμβάνοντας τις ακόλουθες:

noexec

Δεν επιτρέπεται η λειτουργία εκτελέσιμων σε αυτό το σύστημα αρχείων. Αυτό είναι επίσης μια επιλογή ασφαλείας.

nosuid

Δεν λαμβάνονται υπ' όψιν setuid ή setgid flags στο σύστημα αρχείων.

5.6.3. Η Εντολή `umount`

Η εντολή umount(8) παίρνει, ως παράμετρο, ένα εκ των σημείων προσάρτησης, το όνομα μιας συσκευής, ή τις επιλογές `-a` ή `-A`.

Όλοι οι τύποι δέχονται την `-f` για να εξαναγκάσουν σε αποπροσάρτηση, και την `-v` για αναλυτική αναφορά. Σας προειδοποιούμε πως η επιλογή `-f` γενικά δεν είναι καλή ιδέα. Η εξ' αναγκασμού αποπροσάρτηση μπορεί να οδηγήσει σε κατάρρευση τον υπολογιστή ή να καταστρέψει δεδομένα στο σύστημα αρχείων.

Οι `-a` και `-A` χρησιμοποιούνται για να αποπροσαρτήσουν όλα τα προσαρτημένα συστήματα αρχείων, σύμφωνα και με τις επιλογές που δίνονται από το `-t`, αν υπάρχει. Το `-A`, ωστόσο, δεν θα επιχειρήσει να αποπροσαρτήσει το root σύστημα αρχείων.

5.7. Διεργασίες

Το FreeBSD είναι ένα λειτουργικό σύστημα multi-tasking. Αυτό σημαίνει πως κάθε στιγμή μπορούν να τρέχουν παραπάνω από ένα προγράμματα. Κάθε πρόγραμμα που τρέχει οποιαδήποτε στιγμή ονομάζεται *διεργασία* (process). Κάθε εντολή που τρέχετε ξεκινάει τουλάχιστον μία νέα διεργασία, και υπάρχουν κάποιες διεργασίες του συστήματος που τρέχουν συνέχεια για να κρατούν το σύστημα σε λειτουργία.

Κάθε διεργασία χαρακτηρίζεται από ένα μοναδικό αριθμό που ονομάζεται *ID διεργασίας* ή *PID*, και όπως ακριβώς συμβαίνει με τα αρχεία, κάθε διεργασία έχει έναν ιδιοκτήτη και ένα γκρουπ. Οι πληροφορίες του ιδιοκτήτη και του γκρουπ χρειάζονται για να προσδιορίζεται ποια αρχεία και συσκευές μπορεί να ανοίξει η συγκεκριμένη διεργασία, χρησιμοποιώντας τις άδειες αρχείων που συζητήσαμε νωρίτερα. Οι περισσότερες διεργασίες έχουν επίσης μία γονική διεργασία. Η γονική διεργασία είναι εκείνη η διεργασία που τις ξεκίνησε. Για παράδειγμα, εάν πληκτρολογείτε εντολές στο κέλυφος, τότε το κέλυφος είναι μία διεργασία, και κάθε εντολή που τρέχετε είναι επίσης μία διεργασία. Επομένως κάθε διεργασία που τρέχετε με αυτόν τον τρόπο θα έχει γονική διεργασία το κέλυφος σας. Η μόνη εξαίρεση είναι μία διεργασία που ονομάζεται init(8). Η `init` είναι πάντα η πρώτη διεργασία, και επομένως το PID της είναι πάντα 1. Η `init` ξεκινά αυτόματα από τον πυρήνα κατά την εκκίνηση του FreeBSD.

Δύο ιδιαίτερα χρήσιμες εντολές για να παρατηρείτε τις διεργασίες στο σύστημα, είναι οι ps(1) και top(1). Η εντολή `ps` χρησιμοποιείται για την προβολή μιας στατικής λίστας των τρέχοντων

διεργασιών, και μπορεί να εμφανίζει το PID τους, πόση μνήμη χρησιμοποιούν, την εντολή με την οποία ξεκίνησαν, και άλλες πληροφορίες. Η εντολή `top` εμφανίζει όλες τις τρέχουσες διεργασίες, και ανανεώνει την οθόνη σας ανά λίγα δευτερόλεπτα, επομένως μπορείτε να παρατηρείτε τι ακριβώς κάνει ο υπολογιστή σας τη δεδομένη στιγμή.

Η `ps`, από προεπιλογή, εμφανίζει μόνο τις εντολές που τρέχουν και ανήκουν σε εσάς. Για παράδειγμα:

```
% ps
  PID  TT  STAT      TIME COMMAND
  298  p0  Ss     0:01.10 tcsh
 7078  p0  S      2:40.88 xemacs mdoc.xsl (xemacs-21.1.14)
37393  p0  I      0:03.11 xemacs freebsd.dsl (xemacs-21.1.14)
48630  p0  S      2:50.89 /usr/local/lib/netscape-linux/navigator-linux-4.77.bi
48730  p0  IW     0:00.00 (dns helper) (navigator-linux-)
72210  p0  R+     0:00.00 ps
  390  p1  Is     0:01.14 tcsh
 7059  p2  Is+    1:36.18 /usr/local/bin/mutt -y
 6688  p3  IWs    0:00.00 tcsh
10735  p4  IWs    0:00.00 tcsh
20256  p5  IWs    0:00.00 tcsh
  262  v0  IWs    0:00.00 -tcsh (tcsh)
  270  v0  IW+    0:00.00 /bin/sh /usr/X11R6/bin/startx -- -bpp 16
  280  v0  IW+    0:00.00 xinit /home/nik/.xinitrc -- -bpp 16
  284  v0  IW     0:00.00 /bin/sh /home/nik/.xinitrc
  285  v0  S      0:38.45 /usr/X11R6/bin/sawfish
```

Όπως μπορείτε να δείτε σε αυτό το παράδειγμα, η έξοδος από την ps προβάλλεται σε στήλες. `PID` είναι το PID της διεργασίας όπως αναφέραμε νωρίτερα. Τα PID διανέμονται από 1, έως 99999, και όταν υπερβούν το 99999 ξεκινούν από την αρχή (ένα PID δεν μπορεί να αποδοθεί ξανά αν είναι ήδη σε χρήση). Η στήλη `TT` δείχνει το τερματικό (tty) του προγράμματος που εκτελείται, και μπορεί να αγνοηθεί αυτή τη στιγμή δίχως πρόβλημα. Η `STAT` υποδεικνύει την κατάσταση του προγράμματος, και πάλι μπορεί να αγνοηθεί. Η `TIME` είναι η χρονική διάρκεια που το πρόγραμμα απασχολεί την CPU, αυτό συνήθως δεν είναι ο χρόνος εκτέλεσης αφού τα περισσότερα προγράμματα καθυστερούν με άλλες εργασίες πριν απασχολήσουν την CPU. Η τελευταία στήλη, η `COMMAND` είναι η γραμμή εντολής που δόθηκε για να τρέξει το πρόγραμμα.

Η ps(1) υποστηρίζει διάφορες επιλογές για να αλλάξει την γκάμα των πληροφοριών που εμφανίζονται. Μία από τις πιο χρήσιμες επιλογές είναι η `auxww`. Η `a` εμφανίζει πληροφορίες για όλες τις τρέχουσες διεργασίες, όχι μόνο τις δικές σας. Η `u` εμφανίζει το όνομα χρήστη του ιδιοκτήτη της διεργασίας, όπως και τη χρήσης της μνήμης. Η `x` εμφανίζει πληροφορίες σχετικά με τις διεργασίες των δαιμόνων και η `ww` αναγκάζει την ps(1) να εμφανίσει ολόκληρη την εντολή γραμμής για κάθε διεργασία, αφού συνήθως εμφανίζεται κομμένη λόγω του μήκους της που δεν χωρά να εμφανιστεί στην οθόνη.

Η έξοδος της top(1) είναι παρόμοια. Ένα δείγμα εργασίας της μοιάζει σαν αυτή:

```
% top
```

```
last pid: 72257;  load averages:  0.13,  0.09,  0.03    up 0+13:38:33  22:39:10
47 processes:  1 running, 46 sleeping
CPU states: 12.6% user,  0.0% nice,  7.8% system,  0.0% interrupt, 79.7% idle
Mem: 36M Active, 5256K Inact, 13M Wired, 6312K Cache, 15M Buf, 408K Free
Swap: 256M Total, 38M Used, 217M Free, 15% Inuse

  PID USERNAME PRI NICE  SIZE    RES STATE    TIME   WCPU    CPU COMMAND
72257 nik       28   0  1960K  1044K RUN      0:00 14.86%  1.42% top
 7078 nik        2   0 15280K 10960K select   2:54  0.88%  0.88% xemacs-21.1.14
  281 nik        2   0 18636K  7112K select   5:36  0.73%  0.73% XF86_SVGA
  296 nik        2   0  3240K  1644K select   0:12  0.05%  0.05% xterm
48630 nik        2   0 29816K  9148K select   3:18  0.00%  0.00% navigator-linu
  175 root       2   0   924K   252K select   1:41  0.00%  0.00% syslogd
 7059 nik        2   0  7260K  4644K poll     1:38  0.00%  0.00% mutt
...
```

Η έξοδος είναι χωρισμένη σε δύο τομείς. Η κεφαλίδα (οι πέντε πρώτες γραμμές) εμφανίζουν το PID της τελευταίας διεργασίας που έτρεξε, την μέση τιμή φορτίου (είναι μια μέτρηση που δείχνει πόσο απασχολημένο είναι το σύστημα), ο χρόνος λειτουργίας (uptime) του συστήματος (από την τελευταία επανεκκίνηση) και την τρέχουσα ώρα. Τα άλλα στοιχεία στην κεφαλίδα σχετίζονται με το νούμερο των διεργασιών που τρέχουν (47 σε αυτή τη περίπτωση), πόση μνήμη και χώρο swap κατέχουν και πόσο χρόνο ξοδεύει το σύστημα σε διάφορες καταστάσεις λειτουργίας της CPU.

Πιο κάτω ακολουθεί μια σειρά από στήλες, που περιέχουν παρόμοιες πληροφορίες με την έξοδο της ps. Όπως και νωρίτερα μπορείτε να δείτε το PID, το όνομα χρήστη, το ποσοστό χρήσης της CPU, και την εντολή με την οποία ξεκίνησε η διεργασία. Η top(1) από προεπιλογή, εμφανίζει επίσης το ποσοστό μνήμης που χρησιμοποιείται από τη διεργασία. Αυτή χωρίζεται σε δύο στήλες. Η μία είναι για το συνολικό μέγεθος μνήμης που χρειάστηκε η εφαρμογή, ενώ η άλλη για το μέγεθος της μνήμης που καταναλώνει την παρούσα στιγμή. Σε αυτό το παράδειγμα μπορείτε να δείτε ότι ο getenv(3) χρειάστηκε σχεδόν 30 MB RAM, αλλά την παρούσα στιγμή χρησιμοποιεί μόνο 9 MB.

Η top(1) αυτόματα ανανεώνει το περιεχόμενο της κάθε δύο δευτερόλεπτα. Αυτό μπορεί να ρυθμιστεί με την επιλογή s.

5.8. Δαίμονες, Σήματα, και Τερματισμός Διεργασιών

Όταν χρησιμοποιείτε ένα κειμενογράφο, είναι εύκολο να τον ελέγχετε, να φορτώνετε αρχεία, και οτιδήποτε άλλο. Αυτό συμβαίνει διότι ο κειμενογράφος παρέχει αυτές τις δυνατότητες, και επίσης επειδή είναι προσαρτημένος σε ένα *τερματικό*. Μερικά προγράμματα δεν είναι σχεδιασμένα να δουλεύουν με συνεχείς χειρισμούς από τον χρήστη, και επομένως αποσυνδέονται από το τερματικό με την πρώτη ευκαιρία. Για παράδειγμα, ένας εξυπηρετητής web ξοδεύει όλο του το χρόνο στο να απαντά σε αιτήματα web, επομένως δεν χρειάζεται καμιά εισαγωγή δεδομένων από τον χρήστη. Άλλο παραπλήσιο παράδειγμα εφαρμογής, είναι τα προγράμματα μεταφοράς μηνυμάτων ηλεκτρονικής αλληλογραφίας από μια τοποθεσία σε μιαν άλλη.

Ονομάζουμε αυτά τα προγράμματα *δαίμονες (daemons)*. Οι δαίμονες ήταν χαρακτήρες της Ελληνικής μυθολογίας (ούτε καλοί - ούτε κακοί), ήταν απλά μικρά συνοδευτικά πνεύματα που έκαναν χρήσιμα πράγματα για την ανθρωπότητα, όπως ακριβώς και οι διακομιστές web και εξυπηρετητές ηλεκτρονικής αλληλογραφίας σήμερα κάνουν χρήσιμα πράγματα. Αυτός είναι και ο

λόγος για τον οποίο η μασκότ του BSD είναι εδώ και πολύ καιρό ο χαρούμενος δαίμονας με πάνινα σπορ παπούτσια και την τρίαινα.

Η ονομασία των προγραμμάτων που τρέχουν σαν δαίμονες συμβατικά τελειώνει με "d". Το BIND είναι το Berkeley Internet Name Domain, αλλά το πραγματικό πρόγραμμα που τρέχει ονομάζεται `named`, το πρόγραμμα του εξυπηρετητή web Apache λέγεται `httpd`, ο δαίμονας ελέγχου των εκτυπωτών γραμμής είναι ο `lpd` και ούτω καθεξής. Αυτή είναι απλά μια σύμβαση, όχι απόλυτος κανόνας, για παράδειγμα, ο κύριος δαίμονας ηλεκτρονικής αλληλογραφίας για την εφαρμογή Sendmail ονομάζεται `sendmail`, και όχι `maild`, όπως θα ήταν αναμενόμενο.

Μερικές φορές θα χρειαστεί να επικοινωνείτε με τη διεργασία ενός δαίμονα. Ένας τρόπος για να γίνει αυτό είναι στέλνοντας (όπως και σε κάθε εκτελέσιμη διεργασία) *σήματα (signals)*. Υπάρχουν διάφορα σήματα που μπορείτε να στείλετε - μερικά από αυτά έχουν μια συγκεκριμένη σημασία, ενώ άλλα ερμηνεύονται μέσα από την εφαρμογή, και επομένως για να ξέρουμε πως ερμηνεύονται τα σήματα θα πρέπει να διαβάσουμε την τεκμηρίωση της εφαρμογής. Μπορείτε να στείλετε σήμα σε μια διεργασία μόνο αν σας ανήκει. Αν στείλετε σήμα σε μια διεργασία που ανήκει σε κάποιον άλλο με kill(1) ή kill(2), δεν θα σας επιτραπεί. Η μοναδική εξαίρεση σε αυτό, είναι ο χρήστης `root`, που μπορεί να στέλνει σήματα στις διεργασίες οποιουδήποτε άλλου χρήστη του συστήματος.

Το FreeBSD στέλνει επίσης σήματα σε εφαρμογές σε μερικές περιπτώσεις. Αν μία εφαρμογή είναι γραμμένη άσχημα, και προσπαθεί να προσπελάσει μνήμη που δεν της ανήκει, το FreeBSD στέλνει στη διεργασία το σήμα *Segmentation Violation* (`SIGSEGV`). Αν μια εφαρμογή χρησιμοποίησε το σύστημα ειδοποίησης alarm(3) για να ειδοποιηθεί μετά την πάροδο μιας χρονικής περιόδου τότε το FreeBSD θα στείλει το Alarm signal (`SIGALRM`), και ούτω καθ'εξής.

Δύο σήματα μπορούν να χρησιμοποιηθούν για να σταματήσουν μία διαδικασία, το `SIGTERM` και το `SIGKILL`. Το `SIGTERM` είναι ο σωστός τρόπος για να σταματήσουμε μια διαδικασία. Η διεργασία *αντιλαμβάνεται* το σήμα, εκτελεί το σταμάτημα κλείνοντας όλα τα αρχεία αναφοράς (log files), που πιθανώς να είναι ανοιχτά, και γενικώς τελειώνει οτιδήποτε κάνει την συγκεκριμένη χρονική στιγμή πριν σταματήσει. Σε μερικές περιπτώσεις η διεργασία μπορεί να αγνοήσει το `SIGTERM` εάν βρίσκεται στα μισά κάποιας εργασίας που δεν μπορεί να διακοπεί.

Το σήμα `SIGKILL` δεν μπορεί να αγνοηθεί από μία διεργασία. Είναι σαν να λέει στη διεργασία, "Δεν με ενδιαφέρει τι κάνεις, σταμάτα τώρα αμέσως". Αν στείλετε το σήμα `SIGKILL` σε μια διαδικασία τότε το FreeBSD θα σταματήσει την διαδικασία άμεσα .

Άλλα σήματα που πιθανώς να θέλετε να χρησιμοποιήσετε είναι τα `SIGHUP`, `SIGUSR1`, και `SIGUSR2`. Αυτά είναι σήματα γενικής χρήσης, και όταν αποστέλλονται κάνουν διαφορετικά πράγματα ανάλογα με την εφαρμογή.

Ας υποθέσουμε πως αλλάξατε το αρχείο ρύθμισης του εξυπηρετητή διαδικτύου σας, και πως θα θέλατε να πείτε στον εξυπηρετητή να ξαναδιαβάσει τις ρυθμίσεις. Θα μπορούσατε να σταματήσετε και να επανεκκινήσετε το `httpd`, αλλά αυτό θα οδηγούσε σε μια χρονική περίοδο όπου ο εξυπηρετητής θα έμενε εκτός λειτουργίας, κάτι το οποίο μπορεί να είναι ανεπιθύμητο. Οι περισσότεροι δαίμονες είναι σχεδιασμένοι να απαντούν σε σήματα `SIGHUP` για την εκ νέου ανάγνωση του αρχείου ρύθμισης τους. Επομένως, αντί να σταματήσουμε και να επανεκκινήσουμε το `httpd` θα μπορούσαμε να του στείλουμε το σήμα `SIGHUP`. Επειδή δεν υπάρχει συγκεκριμένος τρόπος στην απάντηση αυτών των σημάτων, και διαφορετικοί δαίμονες έχουν διαφορετική συμπεριφορά, πρέπει να διαβάσετε πρώτα την τεκμηρίωση για τον συγκεκριμένο δαίμονα.

Τα σήματα στέλνονται χρησιμοποιώντας την εντολή kill(1), όπως υποδεικνύει το ακόλουθο παράδειγμα.

Procedure: Στέλνοντας Σήμα σε μία Διεργασία

Αυτό το παράδειγμα δείχνει πως να στείλετε σήμα στην inetd(8). Το αρχείο ρύθμισης της `inetd` είναι το /etc/inetd.conf, και η `inetd` θα ξανα-διαβάσει αυτό το αρχείο ρύθμισης όταν θα σταλεί το σήμα `SIGHUP`.

1. Βρείτε το PID της διεργασίας, της οποίας επιθυμείτε να στείλετε το σήμα. Ενεργήστε χρησιμοποιώντας τις εντολές ps(1) και grep(1). Η εντολή grep(1) χρησιμοποιείται για να ψάξει στην έξοδο μιας εντολής, για τους αλφαριθμητικούς χαρακτήρες που έχετε ορίσει. Η εντολή εκτελείται από έναν απλό χρήστη, ενώ η inetd(8) εκτελείται από τον `root`, επομένως θα πρέπει να προσθέσετε την επιλογή `ax` στην ps(1).

   ```
   % ps -ax | grep inetd
     198  ??  IWs    0:00.00 inetd -wW
   ```

   Επομένως το PID της inetd(8) είναι το 198. Σε μερικές περιπτώσεις μπορεί να εμφανίζεται στην έξοδο η εντολή `grep inetd`. Αυτό οφείλεται στον τρόπο με τον οποίο η ps(1) ψάχνει την λίστα των ενεργών διεργασιών.

2. Χρησιμοποιήστε την kill(1) για να στείλετε το σήμα. Επειδή η inetd(8) τρέχει από τον `root` θα πρέπει πρώτα να χρησιμοποιήσετε su(1) για να γίνετε πρώτα `root`.

   ```
   % su
   Password:
   # /bin/kill -s HUP 198
   ```

   Όπως και με τις περισσότερες εντολές στο UNIX®, η kill(1) δεν θα τυπώσει τίποτε στην έξοδο αν η εντολή είχε επιτυχία. Εάν στείλετε ένα σήμα σε μια διεργασία που δεν σας ανήκει θα δείτε `kill: PID: Operation not permitted`. Αν πληκτρολογήσετε λάθος το PID τότε ή θα στείλετε το σήμα σε λάθος διεργασία,κάτι που μπορεί να είναι άσχημο, ή, αν είστε τυχερός, θα έχετε στείλει το σήμα σε ένα PID που δεν χρησιμοποιείται τη συγκεκριμένη στιγμή, και θα δείτε `kill: PID: No such process`.

Γιατί να χρησιμοποιήσετε την εντολή `/bin/kill`;

Πολλά κελύφη παρέχουν την εντολή `kill` ως ενσωματωμένη εντολή. Αυτό σημαίνει πως το κέλυφος θα στείλει το σήμα άμεσα, αντί να τρέξει το /bin/kill. Αυτό μπορεί να είναι πολύ χρήσιμο, αλλά διαφορετικά κελύφη έχουν διαφορετική σύνταξη για τον καθορισμό το όνομα του σήματος που πρέπει να αποσταλεί. Αντί λοιπόν να πρέπει να μάθουμε όλες τις περιπτώσεις ,είναι ευκολότερο απλά να χρησιμοποιούμε την εντολή `/bin/kill ⋯` άμεσα.

Η αποστολή άλλων σημάτων μοιάζει πάρα πολύ, απλά αντικαταστήστε το `TERM` ή το `KILL` στη γραμμή

εντολών με κάποιο άλλο.

Η φόνευση τυχαίων διεργασιών στο σύστημα μπορεί να είναι κακή ιδέα. Ιδιαίτερα, η init(8), με PID 1, είναι πολύ ειδική. Η εκτέλεση της εντολής `/bin/kill -s KILL 1` είναι ένας γρήγορος τρόπος να σβήσετε το σύστημα σας. *Πάντα* να ελέγχετε δύο φορές τις παραμέτρους που χρησιμοποιείτε με την kill(1) *πριν* πιέσετε `Return`.

5.9. Κελύφη

Στο FreeBSD ένα μεγάλο μέρος της καθημερινής εργασίας γίνεται σε ένα περιβάλλον γραμμής εντολών ονόματι κέλυφος (shell). Η κύρια δουλειά του κελύφους είναι να παίρνει εντολές από το κανάλι εισόδου και να τις εκτελεί. Μερικά κελύφη έχουν ενσωματωμένες λειτουργίες ώστε να βοηθούν στις καθημερινές προγραμματισμένες εργασίες όπως διαχείριση αρχείων, file globbing, επεξεργασία γραμμής εντολών, μακροεντολές, και μεταβλητές περιβάλλοντος. Το FreeBSD διατίθεται με διάφορα κελύφη, όπως το `sh`, το Bourne Shell και το `tcsh`, το βελτιωμένο C-shell. Διάφορα άλλα κελύφη είναι διαθέσιμα από την Συλλογή των Ports του FreeBSD, όπως τα `zsh` και `bash`.

Ποιο κέλυφος να χρησιμοποιήσετε; Είναι πραγματικά θέμα γούστου. Εάν είστε προγραμματιστής σε γλώσσα C θα αισθανθείτε περισσότερο οικείος με τα κελύφη τύπου C, όπως το `tcsh`. Εάν έρχεστε από το Linux ή είστε νέος σε περιβάλλον γραμμής εντολών UNIX® μπορείτε να δοκιμάσετε το `bash`. Η ουσία είναι πως κάθε κέλυφος έχει μοναδικές ιδιότητες που μπορεί να συνεργαστούν με το περιβάλλον εργασίας της προτίμησης σας, και επομένως είναι επιλογή σας ποιο κέλυφος να χρησιμοποιήσετε.

Μια κοινή ιδιότητα όλων των κελυφών είναι η αυτόματη συμπλήρωση ονομάτων αρχείων. Αφού έχετε πληκτρολογήσει τα πρώτα γράμματα μιας εντολής ή ενός ονόματος αρχείου αν πιέσετε το πλήκτρο `Tab` στο πληκτρολόγιο, τότε το κέλυφος αυτόματα θα ολοκληρώσει το υπόλοιπο της εντολής ή του ονόματος αρχείου. Ας δώσουμε ένα παράδειγμα. Ας υποθέσουμε πως έχετε δύο αρχεία foobar και foo.bar. Αν θέλετε να σβήσετε το foo.bar θα πρέπει να πληκτρολογήσετε `rm fo[Tab].[Tab]`.

Το κέλυφος θα τυπώσει αυτόματα `rm foo[BEEP].bar`.

Το [BEEP] είναι το κουδούνι της κονσόλας, το οποίο μας πληροφορεί πως δεν ήταν δυνατόν να ολοκληρώσει το όνομα του αρχείου διότι υπάρχουν περισσότερα από ένα ονόματα αρχείων που ταιριάζουν. Όντως το foobar και το foo.bar ξεκινούν με `fo`, και το κέλυφος κατάφερε να συμπληρώσει ως το `foo`. Αν πληκτρολογήσετε επιπλέον `.`, και μετά πάλι `Tab`, το κέλυφος θα καταφέρει να συμπληρώσει το υπόλοιπο του ονόματος αρχείου για σας.

Άλλο ιδιαίτερο χαρακτηριστικό του κελύφους είναι η χρήση των μεταβλητών περιβάλλοντος. Οι μεταβλητές περιβάλλοντος είναι ένα ζεύγος μεταβλητών/κλειδιών αποθηκευμένα στον περιβάλλοντα χώρο του κελύφους Αυτός ο χώρος μπορεί να διαβαστεί από οποιοδήποτε πρόγραμμα που καλείται από το κέλυφος, και έτσι περιέχει πλήθος ρυθμίσεων προγραμμάτων. Ακολουθεί μία λίστα με συνήθεις μεταβλητές περιβάλλοντος και τη σημασία τους:

Μεταβλητή	Περιγραφή
`USER`	Όνομα του τρέχοντα χρήστη.

Μεταβλητή	Περιγραφή
PATH	Λίστα καταλόγων για την αναζήτηση εκτελέσιμων χωρισμένη με άνω-κάτω τελείες.
DISPLAY	Όνομα δικτύου της οθόνης X11 που είναι διαθέσιμη για σύνδεση, αν υπάρχει.
SHELL	Το ενεργό κέλυφος.
TERM	Το όνομα του τύπου του τερματικού χρήστη. Ορίζει τις δυνατότητες του τερματικού.
TERMCAP	Εγγραφή στη βάση δεδομένων κωδικών escape για διάφορες λειτουργίες τερματικών.
OSTYPE	Ο τύπος του λειτουργικού συστήματος π.χ., FreeBSD.
MACHTYPE	Η αρχιτεκτονική CPU στην οποία δουλεύει το σύστημα.
EDITOR	Ο προεπιλεγμένος κειμενογράφος του χρήστη.
PAGER	Το προεπιλεγμένο πρόγραμμα σελιδοποίησης του χρήστη.
MANPATH	Λίστα καταλόγων για την αναζήτηση των σελίδων βοηθείας (man pages) χωρισμένη με άνω-κάτω τελείες.

Ο ορισμός μιας μεταβλητής περιβάλλοντος διαφέρει κάπως από κέλυφος σε κέλυφος. Για παράδειγμα στα κελύφη τύπου-C, όπως τα tcsh και csh, θα πρέπει να χρησιμοποιήσετε την setenv για να ορίσετε μεταβλητές περιβάλλοντος. Σε κελύφη Bourne όπως τα sh και bash, θα πρέπει να χρησιμοποιείτε την export για να θέσετε τις τρέχουσες μεταβλητές περιβάλλοντος. Για παράδειγμα, για να ορίσετε ή να μετατρέψετε την μεταβλητή περιβάλλοντος EDITOR, σε csh ή tcsh θα πρέπει να δώσετε μια εντολή που να θέτει τη μεταβλητή EDITOR στο /usr/local/bin/emacs:

```
% setenv EDITOR /usr/local/bin/emacs
```

Για κελύφη Bourne:

```
% export EDITOR="/usr/local/bin/emacs"
```

Μπορείτε επίσης στα περισσότερα κελύφη να αναπτύσσετε τις μεταβλητές περιβάλλοντος τοποθετώντας μπροστά τους τον χαρακτήρα $. Για παράδειγμα, η echo $TERM θα τυπώσει την τιμή που έχουμε θέσει στην μεταβλητή, διότι το κέλυφος αναπτύσσει την $TERM και περνά την τιμή της στην echo.

Τα κελύφη χρησιμοποιούν μερικούς ειδικούς χαρακτήρες, που ονομάζονται meta-χαρακτήρες για εμφανίσεις ιδιαίτερων δεδομένων. Ο πιο κοινός εξ' αυτών είναι ο χαρακτήρας , ο οποίος αντιπροσωπεύει οποιοδήποτε αλφαριθμητικό χαρακτήρα σε ένα όνομα αρχείου. Αυτοί οι ειδικοί meta-χαρακτήρες μπορούν να χρησιμοποιηθούν για να κάνουν filename globbing. Για παράδειγμα, αν

πληκτρολογήσετε echo * είναι σχεδόν το ίδιο με το να δώσετε ls διότι το κέλυφος παίρνει όλα τα αρχεία που ταιριάζουν με και τα προωθεί στην γραμμή εντολών για την echo.

Για να εμποδίσετε το κέλυφος να επεξεργαστεί αυτούς τους ειδικούς χαρακτήρες, μπορείτε να χρησιμοποιήσετε το σύμβολο διαφυγής (escape) τοποθετώντας μπροστά τους μια δεξιόστροφη κάθετο (\). Η echo $TERM τυπώνει τον τύπο του τερματικού σας, ενώ η echo \$TERM τυπώνει απλά $TERM.

5.9.1. Αλλάζοντας το Κέλυφος σας

Ο ευκολότερος τρόπος για να αλλάξετε το κέλυφος σας είναι να χρησιμοποιήσετε την εντολή chsh. Τρέχοντας την chsh θα οδηγηθείτε στον κειμενογράφο που έχετε θέσει στην μεταβλητή περιβάλλοντος EDITOR, ενώ αν δεν έχετε θέσει, θα οδηγηθείτε στο vi. Αλλάξτε κατάλληλα τη γραμμή "Shell:"

Μπορείτε επίσης να δώσετε στην chsh την επιλογή -s, αυτή θα θέσει το κέλυφος για σας, δίχως να χρειαστεί να χρησιμοποιήσετε τον κειμενογράφο. Για παράδειγμα, αν θέλετε να αλλάξετε το κέλυφος σας σε bash, η ακόλουθη εντολή είναι ακριβώς αυτό που χρειάζεστε:

```
% chsh -s /usr/local/bin/bash
```

Το κέλυφος στο οποίο επιθυμείτε να μεταβείτε *πρέπει* να είναι καταχωρημένο στο αρχείο /etc/shells. Αν έχετε εγκαταστήσει ένα κέλυφος από τη συλλογή των ports, τότε αυτό θα πρέπει να έχει ήδη γίνει. Αν εγκαταστήσατε το κέλυφος μόνοι σας, τότε θα πρέπει να εκτελέσετε τη διαδικασία που ακολουθεί.

Αν για παράδειγμα, εγκαταστήσατε το bash μόνοι σας και το τοποθετήσατε στον /usr/local/bin, τότε θα πρέπει να δώσετε:

```
# echo "/usr/local/bin/bash" >> /etc/shells
```

Και μετά ξανατρέξτε την chsh.

5.10. Κειμενογράφοι

Αρκετές ρυθμίσεις στο FreeBSD γίνονται με επεξεργασία αρχείων κειμένου. Για αυτό το λόγο, θα ήταν καλή ιδέα να εξοικειωθείτε με ένα κειμενογράφο. Αρκετοί περιέχονται στο βασικό σύστημα του FreeBSD και πολλοί περισσότεροι είναι διαθέσιμοι στην Συλλογή των Ports (Ports Collection).

Ο ευκολότερος και απλούστερος κειμενογράφος για να μάθετε ονομάζεται ee, που σημαίνει easy editor (εύκολος κειμενογράφος). Για να ξεκινήσετε τον ee, πρέπει να πληκτρολογήσετε στην γραμμή εντολών ee filename όπου *filename* είναι το όνομα του αρχείου που θέλετε να επεξεργαστείτε. Για παράδειγμα, για να επεξεργαστείτε το /etc/rc.conf, πληκτρολογείτε ee /etc/rc.conf. Μόλις εισέλθετε στο ee, όλες οι εντολές για να χειριστείτε τις λειτουργίες του κειμενογράφου αναφέρονται στο πάνω μέρος της οθόνης. Ο χαρακτήρας καπέλο ^ σημαίνει το πλήκτρο Ctrl, επομένως ^e σημαίνει πως πρέπει να πληκτρολογήσετε τον συνδυασμό πλήκτρων Ctrl + e. Για να βγείτε από το ee, πιέζετε το

πλήκτρο `Esc`, και επιλέγετε leave editor. Ο κειμενογράφος θα σας προτρέψει να σώσετε τυχόν αλλαγές, αν έχετε επεξεργαστεί το αρχείο.

Το FreeBSD παρέχεται επίσης με πιο εξελιγμένους κειμενογράφους όπως το ενσωματωμένο στο βασικό σύστημα vi. Το Emacs και το vim, είναι μέρος της Συλλογής των Ports του FreeBSD (editors/emacs και editors/vim). Αυτοί οι κειμενογράφοι προσφέρουν πολλές περισσότερες λειτουργίες και δυνατότητες, με κόστος αυξημένη πολυπλοκότητα και δυσκολία εκμάθησης. Ωστόσο αν σχεδιάζετε να επεξεργαστείτε αρκετά κείμενα, η εκμάθηση ενός ισχυρού κειμενογράφου όπως το vim ή το Emacs θα σας γλυτώσει πολύ περισσότερο χρόνο επεξεργασίας στην πορεία.

Πολλές εφαρμογές που χρειάζεται να αλλάξουν κάποιο αρχείο ή απαιτούν από το χρήστη να πληκτρολογήσει κάποιο κείμενο, θα ανοίξουν αυτόματα κάποιο κειμενογράφο. Για να αλλάξετε τον προεπιλεγμένο κειμενογράφο, θα πρέπει να θέσετε κατάλληλη τιμή στην μεταβλητή περιβάλλοντος `EDITOR`. Δείτε την ενότητα Κελύφη για περισσότερες λεπτομέρειες.

5.11. Συσκευές και Αρχεία συσκευών

Συσκευή είναι ένας όρος που αναφέρεται σε σχέση με λειτουργίες hardware ενός συστήματος, περιλαμβάνοντας δίσκους, εκτυπωτές, κάρτες γραφικών και πληκτρολόγια. Κατά την εκκίνηση του FreeBSD οι περισσότερες πληροφορίες που αναγράφονται στην οθόνη είναι συσκευές που αναγνωρίζονται από το σύστημα. Μπορείτε να ξαναδείτε τα μηνύματα εκκίνησης, διαβάζοντας το /var/run/dmesg.boot.

Για παράδειγμα, acd0 είναι ο πρώτος οδηγός IDE CDROM, ενώ το kbd0 αντιπροσωπεύει το πληκτρολόγιο.

Στις περισσότερες από αυτές τις συσκευές σε ένα λειτουργικό σύστημα UNIX® η πρόσβαση πρέπει να γίνεται διαμέσου ειδικών αρχείων που ονομάζονται αρχεία συσκευών, και είναι τοποθετημένα στον κατάλογο /dev.

5.11.1. Δημιουργώντας Αρχεία Συσκευών

Όταν προσθέτετε μια νέα συσκευή στο σύστημα σας, ή μεταγλωττίζετε πηγαίο κώδικα για υποστήριξη νέων οδηγών, πρέπει να δημιουργούνται νέα αρχεία συσκευών.

5.11.1.1. `DEVFS` (DEVice File System)

Το σύστημα αρχείων συσκευών ή, `DEVFS`, παρέχει πρόσβαση στο χώρο ονομάτων συσκευών του πυρήνα (device namespace) στο global σύστημα αρχείων του συστήματος. Αντί να δημιουργείτε και να μετατρέπετε αρχεία συσκευών, το `DEVFS` συντηρεί για σας αυτό το ιδιαίτερο σύστημα αρχείων.

Δείτε την σελίδα βοηθείας devfs(5) για περισσότερες πληροφορίες.

5.12. Τύποι Εκτελέσιμων

Για να καταλάβετε γιατί το FreeBSD χρησιμοποιεί τον τύπο elf(5) θα πρέπει πρώτα να γνωρίζετε μερικά πράγματα για τους τρεις "κυρίαρχους" τύπους εκτελέσιμων για το UNIX®

- a.out(5)

Ο παλαιότερος και πιο "κλασσικός" τύπος αντικειμένων του UNIX®. Χρησιμοποιεί μια μικρή και συμπαγή κεφαλίδα με ένα μαγικό νούμερο στην αρχή που συχνά χρησιμοποιείται για να χαρακτηρίζει τον τύπο (δείτε για περισσότερες πληροφορίες την a.out(5)). Περιέχει τρία φορτωμένα τμήματα: .text, .data και .bss και επιπλέον ένα πίνακα συμβόλων και ένα πίνακα αλφαριθμητικών χαρακτήρων.

- COFF

  Ο τύπος αντικειμένου SVR3. Η κεφαλίδα τώρα αποτελείται από ένα πίνακα τομέων, ώστε να μπορούμε να έχουμε κάτι παραπάνω από απλά .text, .data και .bss.

- elf(5)

  Ο διάδοχος του COFF, περιλαμβάνει πολλαπλά τμήματα και δέχεται τιμές 32 ή 64 bit. Το βασικό μειονέκτημα: Ο ELF σχεδιάστηκε με την προϋπόθεση πως θα υπήρχε μόνο ένα ABI για κάθε αρχιτεκτονική συστήματος. Αυτή η υπόθεση είναι όμως εσφαλμένη τώρα, αφού ακόμη και στον εμπορικό κόσμο του SYSV (όπου υπάρχουν τουλάχιστον τρία ABI: SRV4, Solaris, SCO) δεν ισχύει.

  Το FreeBSD προσπαθεί να ξεπεράσει αυτό το πρόβλημα παρέχοντας ένα βοηθητικό πρόγραμμα με το οποίο μπορούμε να *ενσωματώσουμε (branding)* σε ένα εκτελέσιμο ELF τις πληροφορίες για το ABI που είναι συμβατό με αυτό. Δείτε την σελίδα manual του brandelf(1) για περισσότερες πληροφορίες.

Το FreeBSD προέρχεται από τον "κλασσικό" χώρο και μέχρι την αρχή της σειράς 3.X, χρησιμοποιούσε τον τύπο a.out(5), μια τεχνολογία δοκιμασμένη και αποδεδειγμένη σε πολλές γενιές εκδόσεων του BSD. Αν και η μεταγλώττιση και εκτέλεση εγγενών εκτελέσιμων (και πυρήνων) τύπου ELF ήταν δυνατή στα FreeBSD συστήματα ήδη από πολύ καιρό πριν, το FreeBSD αρχικά αντιστάθηκε στην "ώθηση" για καθιέρωση του ELF ως προκαθορισμένου τύπου. Γιατί; Όταν ο κόσμος του Λίνουξ έκανε την οδυνηρή μετάβαση προς το ELF, δεν ήταν τόσο για να ξεφύγει από τον τύπο εκτελέσιμων a.out όσο για να αντιμετωπίσει το δύσκαμπτο δικό τους μηχανισμό κοινόχρηστων βιβλιοθηκών, ο οποίος βασίζονταν σε jump-tables και προκαλούσε μεγάλη δυσχέρεια στην κατασκευή τους, τόσο στους προγραμματιστές όσο και στους μεταπωλητές. Από τη στιγμή που τα διαθέσιμα εργαλεία του ELF προσέφεραν λύση στο πρόβλημα των κοινών βιβλιοθηκών και έγινε γενικώς αποδεκτό πως ήταν "ο δρόμος προς τα εμπρός", έγινε αποδεκτό το αναγκαίο κόστος της μεταφοράς και επιτεύχθηκε η μετακίνηση. Ο μηχανισμός κοινόχρηστων βιβλιοθηκών του FreeBSD βασίζεται σε μεγάλο βαθμό στον αντίστοιχο μηχανισμό του SunOS™ της Sun και είναι πολύ εύκολος στη χρήση.

Τότε, γιατί υπάρχουν τόσοι διαφορετικοί τύποι;

Πίσω στο σκοτεινό παρελθόν, υπήρχε απλό hardware. Αυτό το απλό hardware υποστήριζε ένα απλό, μικρό σύστημα. Το a.out ήταν απόλυτα κατάλληλο για την αναπαράσταση εκτελέσιμων σε αυτό το απλό σύστημα (ένα PDP-11). Όταν ο κόσμος άρχισε να μεταφέρει το UNIX® από αυτό το απλό σύστημα, διατηρήθηκε ο τύπος a.out γιατί ήταν ικανοποιητικός για τα πρώτα ports του UNIX® σε αρχιτεκτονικές όπως η Motorola 68k, VAXen, κτλ.

Μετέπειτα κάποιος λαμπρός μηχανικός hardware αποφάσισε πως αφού μπορούσε να εξαναγκάζει το λογισμικό να κάνει τόσα πρόχειρα κόλπα, θα μπορούσε επίσης να παραλείψει μερικές πύλες από το σχεδιασμό ώστε να επιτρέψει στον πυρήνα της CPU να τρέχει γρηγορότερα. Αν και διασκευάσθηκε ώστε να δουλεύει με αυτό το νέο είδος hardware (γνωστό σήμερα ως RISC), ο τύπος

a.out ήταν τελικά ακατάλληλος για αυτό, και έτσι σχεδιάστηκαν πολλοί νέοι τύποι για να επιτευχθεί καλύτερη απόδοση από το hardware από ότι ήταν δυνατόν με τον απλό και περιοριστικό τύπο a.out. Εφευρέθηκαν διάφοροι τύποι όπως οι COFF, ECOFF, και μερικοί άλλοι λιγότερο γνωστοί, και ερευνήθηκαν οι περιορισμοί τους ώσπου τα πράγματα σταθεροποιήθηκαν στο ELF.

Επιπλέον, το μέγεθος των προγραμμάτων γινόταν όλο και μεγαλύτερο και οι δίσκοι (και η φυσική μνήμη) ήταν ακόμη σχετικά μικροί και κάπως έτσι γεννήθηκε η ιδέα της κοινής βιβλιοθήκης. Το σύστημα VM έγινε επίσης περισσότερο περίπλοκο. Κάθε μία από τις βελτιώσεις γινόταν με βάση τον τύπο a.out, που όμως γινόταν όλο και πιο δύσχρηστος με κάθε νέα προσθήκη. Επιπρόσθετα, ο κόσμος ήθελε να φορτώνει τμήματα δυναμικά ενώ το σύστημα ήταν σε φάση εκτέλεσης, ή να εξαλείφει μέρη προγραμμάτων αφού είχε εκτελεστεί ο κώδικας αρχικοποίησης (init) ώστε να εξοικονομηθεί φυσική μνήμη και χώρος swap. Οι γλώσσες προγραμματισμού γινόντουσαν ακόμα πιο περίπλοκες και ο κόσμος ήθελε αυτόματη φόρτωση και εκτέλεση κώδικα πριν την κλήση της main. Έγιναν πρόχειρες διορθώσεις (hacks) στον τύπο a.out ώστε να συμβαδίζει με όλες αυτές τις αλλαγές, και πράγματι, για μια περίοδο έδειχνε να λειτουργεί. Με τον καιρό όμως, φάνηκε ότι ο τύπος a.out δεν θα μπορούσε να αντεπεξέλθει σε όλα αυτά τα προβλήματα, αφού θα έπρεπε να αναπτύσσεται συνεχώς και με περίπλοκο τρόπο. Αν και το ELF έλυνε πολλά από αυτά τα προβλήματα, η μετάβαση σε αυτό ενός συστήματος που βασικά λειτουργούσε, θα οδηγούσε σε οδυνηρές καταστάσεις. Έτσι ο τύπος ELF έπρεπε να περιμένει μέχρι τη στιγμή όπου η παραμονή στο a.out θα δημιουργούσε περισσότερα προβλήματα από ότι η μετάβαση στο ELF.

Ωστόσο, όσο ο καιρός περνούσε, και τα εργαλεία μεταγλώττισης από τα οποία προέρχονται τα αντίστοιχα εργαλεία του FreeBSD (ειδικότερα ο assembler και ο loader), αναπτύχθηκαν παράλληλα σε δύο δέντρα. Το δέντρο του FreeBSD πρόσθεσε κοινές βιβλιοθήκες και διόρθωσε κάποια σφάλματα. Η ομάδα του GNU που είχε αρχικά γράψει αυτά τα προγράμματα, τα έγραψε ξανά και πρόσθεσε ευκολότερη υποστήριξη για κατασκευή cross compilers, την ενσωμάτωση διαφορετικών τύπων κατά βούληση, κλπ. Αν και πολλοί ζητούσαν να κατασκευαστούν cross compilers για FreeBSD, ήταν άτυχοι, αφού ο παλιός πηγαίος κώδικας του FreeBSD για τα as και ld τα έκανε ακατάλληλα. Η νέα αλυσίδα εργαλείων του GNU (binutils) υποστηρίζει cross compiling, ELF, κοινές βιβλιοθήκες, προεκτάσεις C++, κτλ. Επιπλέον, πολλοί τρίτοι κατασκευαστές προσφέρουν εκτελέσιμα ELF, και είναι πολύ καλό να μπορούν να εκτελεστούν στο FreeBSD.

Ο ELF είναι πιο εκφραστικός από τον a.out και περισσότερο επεκτάσιμος στο βασικό σύστημα. Τα εργαλεία ELF είναι ευκολότερα στην συντήρηση και προσφέρουν υποστήριξη για cross compilers, κάτι που είναι πολύ σημαντικό για μερικούς ανθρώπους. Μπορεί ο ELF να είναι λίγο πιο αργός από τον a.out, αλλά η διαφορά δεν είναι αισθητή. Υπάρχουν επίσης πολλές άλλες διαφορές μεταξύ τους, σε λεπτομέρειες όπως τον τρόπο που αντιστοιχίζουν σελίδες, που χειρίζονται τον κώδικα init, κλπ. Καμιά από αυτές δεν είναι πολύ σημαντική, αλλά ωστόσο δεν παύουν να είναι διαφορές. Με τον καιρό η υποστήριξη για το a.out θα απομακρυνθεί από τον πυρήνα GENERIC, και τελικά θα αφαιρεθεί εντελώς από τον πυρήνα όταν εκλείψει ολοκληρωτικά η ανάγκη εκτέλεσης παλαιών προγραμμάτων τύπου a.out.

5.13. Για Περισσότερες Πληροφορίες

5.13.1. Σελίδες Βοηθείας

Η πιο κατανοητή τεκμηρίωση στο FreeBSD προσφέρεται με τη μορφή των σελίδων βοηθείας (manual pages). Σχεδόν για κάθε πρόγραμμα του συστήματος δίνεται μια σύντομη αναφορά που

εξηγεί τις βασικές λειτουργίες και διάφορα άλλα θέματα. Αυτές οι σελίδες προβάλλονται με την εντολή `man`. Η χρήση της εντολής `man` είναι απλή:

```
% man command
```

όπου `command` είναι το όνομα της εντολής για την οποία επιθυμείτε να μάθετε περισσότερες πληροφορίες. Για παράδειγμα, για να μάθετε περισσότερα για την εντολή `ls` πληκτρολογήστε:

```
% man ls
```

Το online manual χωρίζεται σε τέσσερις αριθμημένες ενότητες:

1. Εντολές χρήστη.
2. Κλήσεις συστήματος και αριθμοί σφαλμάτων.
3. Συναρτήσεις των βιβλιοθηκών της C.
4. Οδηγοί συσκευών.
5. Τύποι αρχείων.
6. Παιχνίδια και άλλες εφαρμογές διασκέδασης.
7. Διάφορες πληροφορίες.
8. Συντήρηση συστήματος και εντολές λειτουργίας.
9. Ανάπτυξη πυρήνα.

Σε μερικές περιπτώσεις, το ίδιο θέμα μπορεί να εμφανίζεται σε περισσότερες ενότητες των σελίδων βοηθείας. Για παράδειγμα, υπάρχει η εντολή χρήστη `chmod` και η κλήση συστήματος `chmod()`. Σε αυτή τη περίπτωση, μπορείτε να πείτε στην εντολή `man` ποια ακριβώς θέλετε επιλέγοντας την ενότητα:

```
% man 1 chmod
```

Με αυτόν τον τρόπο θα εμφανιστεί η σελίδα βοηθείας για την εντολή χρήστη `chmod`. Οι αναφορές σε μια ειδική ενότητα των σελίδων βοηθείας τοποθετούνται παραδοσιακά μέσα σε παρένθεση στην τυπωμένη τεκμηρίωση, επομένως το chmod(1) αναφέρεται στην εντολή χρήστη `chmod` και το chmod(2) αναφέρεται στην κλήση συστήματος.

Αυτό είναι χρήσιμο όταν γνωρίζουμε το όνομα της εντολής και απλά επιθυμούμε να μάθουμε πως να την χρησιμοποιήσουμε, αλλά τι γίνεται αν δεν γνωρίζουμε το όνομα της; Μπορείτε να χρησιμοποιήσετε το `man` για να αναζητήσετε λέξεις κλειδιά από τις περιγραφές των εντολών χρησιμοποιώντας την επιλογή `-k`:

```
% man -k mail
```

Με την εντολή αυτή θα εμφανιστεί μία λίστα από εντολές που περιέχουν την λέξη κλειδί "mail" στην περιγραφή τους. Αυτό είναι αντίστοιχο με το να χρησιμοποιήσετε την εντολή `apropos`.

Επομένως, βλέπετε όλες αυτές τις γουστόζικες εντολές στον /usr/bin αλλά δεν έχετε την παραμικρή ιδέα του τι πραγματικά κάνουν; Απλά πληκτρολογήστε:

```
% cd /usr/bin
% man -f *
```

ή

```
% cd /usr/bin
% whatis *
```

το οποίο κάνει ακριβώς το ίδιο πράγμα.

5.13.2. GNU Info Files

Το FreeBSD περιλαμβάνει πολλές εφαρμογές και βοηθητικά προγράμματα που έχουν δημιουργηθεί από την Free Software Foundation (FSF). Πέρα από τις σελίδες βοηθείας, τα προγράμματα αυτά παρέχονται με τεκμηρίωση μορφής hypertext σε αρχεία που ονομάζονται `info` και τα οποία μπορείτε να προβάλλετε με την εντολή `info` ή, αν έχετε εγκαταστήσει το emacs, μέσω της κατάστασης λειτουργίας info mode του emacs.

Για να χρησιμοποιήσετε την εντολή info(1), απλά πληκτρολογήστε:

```
% info
```

Για μια σύντομη εισαγωγή, πληκτρολογήστε `h`. Για μια γρήγορη αναφορά εντολής, πληκτρολογήστε `?`.

Chapter 6. Εγκατάσταση Εφαρμογών: Πακέτα και Ports

6.1. Σύνοψη

Το FreeBSD συνοδεύεται από μία πλούσια συλλογή από προγράμματα σαν μέρος του βασικού συστήματος. Όμως, λίγα μπορεί να κάνει κάποιος πριν βρεθεί στην ανάγκη να εγκαταστήσει μια πρόσθετη εφαρμογή για να υλοποιήσει μια πραγματική εργασία. Το FreeBSD παρέχει δυο συμπληρωματικές τεχνολογίες για να εγκαταστήσετε πρόσθετες εφαρμογές στο σύστημα σας: τη Συλλογή των Ports (Ports Collection, για εγκατάσταση από τον πηγαίο κώδικα), και τα πακέτα (packages, για εγκατάσταση από προ-μεταγλωττισμένα εκτελέσιμα πακέτα). Κάθε μία από τις δυο μεθόδους μπορεί να χρησιμοποιηθεί για να εγκαταστήσετε τις νεότερες εκδόσεις από τις αγαπημένες σας εφαρμογές, από τοπικά αποθηκευτικά μέσα ή απευθείας από το δίκτυο.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να εγκαθιστάτε προ-μεταγλωττισμένα πακέτα λογισμικού.
- Πως να μεταγλωττίζετε πρόσθετο λογισμικό από τον πηγαίο κώδικα χρησιμοποιώντας την Συλλογή των Ports.
- Πως να κάνετε απεγκατάσταση εγκαταστημένων πακέτων ή ports.
- Πως να αλλάζετε τις προκαθορισμένες ρυθμίσεις που χρησιμοποιεί η Συλλογή των Ports.
- Πως να βρίσκετε τα κατάλληλα πακέτα λογισμικού.
- Πως να αναβαθμίζετε τις εφαρμογές σας.

6.2. Επισκόπηση της εγκατάστασης λογισμικού

Αν έχετε χρησιμοποιήσει ένα UNIX® σύστημα στο παρελθόν, θα γνωρίζετε ότι η συνηθισμένη διαδικασία για την εγκατάσταση πρόσθετου λογισμικού είναι περίπου η παρακάτω:

1. "Κατέβασμα" του λογισμικού, που μπορεί να διανέμεται σε μορφή πηγαίου κώδικα, ή σαν εκτελέσιμο.
2. Αποσυμπίεση του λογισμικού από την μορφή της διανομής του (συνήθως ένα tarball συμπιεσμένο με το compress(1), gzip(1), ή bzip2(1)).
3. Εντοπισμός της τεκμηρίωσης (πιθανώς ένα αρχείο INSTALL ή README ή μερικά αρχεία μέσα σε ένα υποκατάλογο doc/) και ανάγνωσή τους για το πως θα εγκατασταθεί το λογισμικό.
4. Αν το λογισμικό διανέμεται με τη μορφή πηγαίου κώδικα, μεταγλώττιση του. Αυτό μπορεί να περιλαμβάνει την επεξεργασία ενός Makefile, ή την εκτέλεση ενός `configure` script, και άλλες εργασίες.
5. Δοκιμή και εγκατάσταση του λογισμικού.

Και αυτά μόνο αν όλα πάνε καλά. Αν εγκαθιστάτε ένα λογισμικό που δεν έχει μεταφερθεί στο FreeBSD ίσως να πρέπει να τροποποιήσετε τον πηγαίο κώδικα για να δουλέψει σωστά.

Αν το θέλετε, μπορείτε να συνεχίσετε να εγκαθιστάτε λογισμικό με τον "παραδοσιακό" τρόπο στο FreeBSD. Όμως, το FreeBSD παρέχει δυο τεχνολογίες που μπορούν να σας γλιτώσουν από πολύ κόπο: τα πακέτα και τα ports. Την στιγμή που γράφτηκε αυτό το κείμενο, διατίθονταν με αυτόν τον τρόπο πάνω από 36000 πρόσθετες εφαρμογές.

Για οποιαδήποτε εφαρμογή, το αντίστοιχο FreeBSD πακέτο της είναι ένα μοναδικό αρχείο που πρέπει εσείς να "κατεβάσετε". Το πακέτο περιέχει προ-μεταγλωττισμένα αντίγραφα από όλες τις εντολές της εφαρμογής, όπως επίσης και αρχεία παραμετροποίησης ή τεκμηρίωσης. Ένα τέτοιο πακέτο σε μορφή αρχείου, μπορείτε να το χειριστείτε με τις εντολές διαχείρισής πακέτων του FreeBSD, όπως οι pkg_add(1), pkg_delete(1), pkg_info(1), και πάει λέγοντας. Η εγκατάσταση μιας νέας εφαρμογής μπορεί να γίνει με μία μόνο εντολή.

Ένα FreeBSD port για μία εφαρμογή είναι μια συλλογή από αρχεία σχεδιασμένα για να αυτοματοποιήσουν την διαδικασία μεταγλώττισης της εφαρμογής από τον πηγαίο κώδικα.

Θυμηθείτε ότι υπάρχουν μερικά βήματα που θα πρέπει λογικά να κάνετε αν μεταγλωττίσετε ένα πρόγραμμα μόνος σας ("κατέβασμα", αποσυμπίεση, προσαρμογή (patching), μεταγλώττιση, εγκατάσταση). Τα αρχεία που αποτελούν ένα port περιέχουν όλες τις απαραίτητες πληροφορίες για να επιτρέψουν στο σύστημα να κάνει όλα αυτά για εσάς. Εσείς εκτελείτε μερικές απλές εντολές, και ο πηγαίος κώδικας για την εφαρμογή αυτόματα "κατεβαίνει", αποσυμπιέζεται, προσαρμόζεται, μεταγλωττίζεται, και εγκαθίσταται για εσάς.

Στην πραγματικότητα, το σύστημα ports μπορεί επίσης να χρησιμοποιηθεί για να δημιουργηθούν πακέτα που μπορείτε αργότερα να διαχειριστείτε με την `pkg_add` και τις άλλες εντολές διαχείρισής πακέτων που θα αναφερθούν σε λίγο.

Τόσο τα πακέτα, όσο και τα ports κατανοούν τις *εξαρτήσεις (dependencies)*. Ας υποθέσουμε ότι θέλετε να εγκαταστήσετε μία εφαρμογή που εξαρτάται από μία συγκεκριμένη βιβλιοθήκη για να λειτουργήσει. Τόσο η εφαρμογή, όσο και η βιβλιοθήκη διατίθενται ως πακέτα και ports του FreeBSD. Αν χρησιμοποιήσετε την εντολή `pkg_add` ή το σύστημα των ports για να εγκαταστήσετε την εφαρμογή, αμφότερα θα παρατηρήσουν ότι η βιβλιοθήκη δεν είναι εγκατεστημένη, και αυτόματα θα την εγκαταστήσουν πριν από το πρόγραμμα.

Έχοντας αναφέρει ότι οι δύο τεχνολογίες είναι αρκετά όμοιες, ίσως να αναρωτιέστε γιατί το FreeBSD προσφέρει και τις δύο. Τα πακέτα και τα ports αμφότερα έχουν τα δικά τους πλεονεκτήματα, και το τι θα χρησιμοποιήσετε εξαρτάται από την δική σας προτίμηση.

Πλεονεκτήματα των Πακέτων

- Ένα συμπιεσμένο tarball πακέτου είναι συνήθως μικρότερο από το συμπιεσμένο tarball που περιέχει τον πηγαίο κώδικα για την εφαρμογή.
- Τα πακέτα δεν χρειάζονται μεταγλώττιση. Για μεγάλες εφαρμογές, όπως είναι ο Mozilla, το KDE, ή το GNOME αυτό μπορεί να είναι σημαντικό, ιδιαίτερα αν βρίσκεστε σε ένα αργό μηχάνημα.
- Τα πακέτα δεν απαιτούν να κατανοήσετε την διαδικασία που σχετίζεται με την μεταγλώττιση λογισμικού στο FreeBSD.

Πλεονεκτήματα των Ports

- Τα πακέτα συνήθως είναι μεταγλωττισμένα με συντηρητικές επιλογές, επειδή πρέπει να λειτουργούν στον μέγιστο αριθμό συστημάτων. Με εγκατάσταση από το port, μπορείτε να

ρυθμίσετε τις επιλογές μεταγλώττισης (για παράδειγμα) να δημιουργήσουν εκτελέσιμο κώδικα που να εκμεταλλεύεται τις ικανότητες ενός Pentium 4 ή Athlon επεξεργαστή.

- Μερικές εφαρμογές έχουν επιλογές μεταγλώττισης που σχετίζονται με το τι μπορούν να κάνουν και τι όχι. Για παράδειγμα, ο Apache μπορεί να μεταγλωττιστεί με ένα ευρύ φάσμα από επιλογές. Μεταγλωττίζοντας τον από το port, δεν είναι ανάγκη να δεχτείτε τις προεπιλεγμένες επιλογές, μπορείτε να κάνετε τις δικές σας.

  Σε μερικές περιπτώσεις, μπορεί να υπάρχουν πολλαπλά πακέτα για την ίδια εφαρμογή, με διαφορετικές ρυθμίσεις. Για παράδειγμα, το Ghostscript διατίθεται ως ένα πακέτο ghostscript και ένα πακέτο ghostscript-nox11, αναλόγως αν θα εγκαταστήσετε ή όχι έναν X11 server. Αυτού του τύπου οι ρυθμίσεις είναι δυνατές με τα πακέτα, αλλά γρήγορα γίνονται αδύνατες αν μία εφαρμογή έχει περισσότερες από μία ή δύο διαφορετικές ρυθμίσεις μεταγλώττισης.

- Οι συνθήκες των αδειών διανομής από μερικές διανομές λογισμικού, απαγορεύουν την διανομή εκτελέσιμου κώδικα. Πρέπει να διανεμηθούν με την μορφή πηγαίου κώδικα.
- Μερικά άτομα δεν εμπιστεύονται τα έτοιμα εκτελέσιμα. Τουλάχιστον με τον πηγαίο κώδικα, μπορείτε (θεωρητικά) να τον διαβάσετε και να ψάξετε για πιθανά προβλήματα μόνος σας.
- Αν έχετε τοπικά, δικά σας patches, θα χρειαστείτε τον πηγαίο κώδικα για να τα εφαρμόσετε.
- Μερικά άτομα γουστάρουν να έχουν τον πηγαίο κώδικα, ώστε να τον διαβάσουν αν βαρεθούνε, να τον αλλάξουν (hack), να δανειστούν από αυτόν (αν βέβαια το επιτρέπει η άδεια), κ.λ.π.

Για να είστε ενήμερος για τα ανανεωμένα ports, εγγραφείτε στην ηλεκτρονική λίστα των FreeBSD ports και στην ηλεκτρονική λίστα αναφορών προβλημάτων των FreeBSD ports.

Πριν εγκαταστήσετε οποιοδήποτε εφαρμογή, πρέπει να ελέγχετε το http://vuxml.freebsd.org/ για θέματα ασφαλείας που σχετίζονται με την εφαρμογή σας.

Μπορείτε επίσης να εγκαταστήσετε το ports-mgmt/portaudit το οποίο αυτόματα θα ελέγχει όλες τις εγκαταστημένες εφαρμογές για γνωστά τρωτά σημεία. Έλεγχος επίσης θα πραγματοποιείται πριν τη μεταγλώττιση οποιουδήποτε port. Στο ενδιάμεσο, μπορείτε να χρησιμοποιείτε την εντολή `portaudit -F -a` αφότου έχετε πρώτα εγκαταστήσει μερικά πακέτα.

Το υπόλοιπο αυτού του κεφαλαίου εξηγεί πως να χρησιμοποιήσετε τα πακέτα και τα ports για να εγκαταστήσετε και να διαχειριστείτε πρόσθετο λογισμικό στο FreeBSD.

6.3. Βρίσκοντας την Εφαρμογή σας

Πριν εγκαταστήσετε οποιαδήποτε εφαρμογή πρέπει να γνωρίζετε τι θέλετε να κάνει, και πως ονομάζεται η εφαρμογή.

Η λίστα των διαθέσιμων εφαρμογών στο FreeBSD μεγαλώνει συνεχώς. Ευτυχώς, υπάρχουν πολλοί τρόποι να βρείτε αυτό που θέλετε:

- Στη δικτυακή τοποθεσία του FreeBSD θα βρείτε μια λίστα από όλες τις διαθέσιμες εφαρμογές, στο http://www.FreeBSD.org/ports/. Η λίστα αυτή ανανεώνεται συχνά, ενώ υπάρχει και

δυνατότητα αναζήτησης. Τα ports είναι χωρισμένα σε κατηγορίες, και μπορείτε να αναζητήσετε μία εφαρμογή είτε με το όνομα (αν το ξέρετε), ή να δείτε όλες τις εφαρμογές που είναι διαθέσιμες σε μια κατηγορία. *

Ο Dan Langille διατηρεί το FreshPorts, στο http://www.FreshPorts.org/. Το FreshPorts καταγράφει τις αλλαγές των εφαρμογών στο δέντρο των ports καθώς συμβαίνουν, επιτρέποντάς σας να "παρακολουθείτε" ένα ή περισσότερα ports, και μπορεί να σας στείλει email όταν αυτά ανανεώνονται. *

Αν δεν γνωρίζετε το όνομα της εφαρμογής που θέλετε, δοκιμάστε να χρησιμοποιήσετε ένα site σαν το Freecode(http://www.freecode.com/) για να βρείτε μία εφαρμογή, και μετά μπορείτε να ελέγξετε ξανά το site του FreeBSD για να δείτε αν η εφαρμογή έχει γίνει port.

- Αν ξέρετε το ακριβές όνομα του port, και θέλετε μόνο να βρείτε σε ποια κατηγορία είναι, μπορείτε να χρησιμοποιήσετε την εντολή whereis(1). Απλά γράψτε `whereis αρχείο`, όπου *αρχείο* είναι το πρόγραμμα που θέλετε να εγκαταστήσετε. Αν αυτό βρίσκεται στο σύστημα σας, η εντολή θα σας πει που είναι, όπως παρακάτω:

```
# whereis lsof
lsof: /usr/ports/sysutils/lsof
```

Αυτό μας λέει ότι το `lsof` (ένα εργαλείο συστήματος) μπορεί να βρεθεί στον κατάλογο /usr/ports/sysutils/lsof.

- Επιπρόσθετα, μπορείτε να χρησιμοποιήσετε μια απλή εντολή echo(1) για να εντοπίσετε την τοποθεσία κάποιου προγράμματος μέσα στα ports. Για παράδειγμα:

```
# echo /usr/ports/*/*lsof*
/usr/ports/sysutils/lsof
```

Σημειώστε ότι το παραπάνω θα δείξει επίσης και οποιαδήποτε αρχεία έχουν κατέβει στον κατάλογο /usr/ports/distfiles εφόσον ταιριάζουν στην αναζήτηση.

- Ακόμη ένας τρόπος να βρείτε ένα συγκεκριμένο port, είναι χρησιμοποιώντας τον εσωτερικό μηχανισμό αναζήτησης της Συλλογής των Ports. Γα να χρησιμοποιήσετε αυτό τον τρόπο αναζήτησης, Θα χρειαστεί να βρίσκεστε στον κατάλογο /usr/ports. Όταν βρεθείτε σε αυτόν τον κατάλογο, εκτελέστε το `make search name=όνομα-προγράμματος` όπου *όνομα—προγράμματος* είναι το όνομα του προγράμματος που θέλετε να βρείτε. Για παράδειγμα, αν αναζητάτε το `lsof`:

```
# cd /usr/ports
# make search name=lsof
Port:   lsof-4.56.4
Path:   /usr/ports/sysutils/lsof
Info:   Lists information about open files (similar to fstat(1))
Maint:  obrien@FreeBSD.org
Index:  sysutils
B-deps:
```

```
R-deps:
```

Το τμήμα της εξόδου που πρέπει να προσέξετε ιδιαίτερα είναι η γραμμή "Path:", αφού αυτή σας λέει που να βρείτε το port. Οι υπόλοιπες πληροφορίες που παρέχονται δεν χρειάζονται για να εγκατασταθεί το port, για αυτό δεν θα αναλυθούν εδώ.

Για πιο λεπτομερή αναζήτηση μπορείτε να χρησιμοποιήσετε επίσης `make search key=φράση` όπου *φράση* είναι κάποιο κείμενο προς αναζήτηση. Αυτό αναζητά ονόματα port, σχόλια, περιγραφές και εξαρτήσεις, και μπορεί να χρησιμοποιηθεί για να βρεθούν ports που σχετίζονται με ένα συγκεκριμένο θέμα, εάν δεν γνωρίζετε το όνομα του προγράμματος που αναζητάτε.

Σε όλες τις παραπάνω περιπτώσεις, η φράση προς αναζήτηση είναι case-insensitive (δεν λαμβάνει υπόψη τις διαφορές κεφαλαίων-μικρών). Η αναζήτηση για το "LSOF", θα δώσει τα ίδια αποτελέσματα με την αναζήτηση για το "lsof".

6.4. Χρησιμοποιώντας το Σύστημα των Πακέτων

Υπάρχουν διάφορα εργαλεία με τα οποία μπορείτε να διαχειριστείτε τα πακέτα στο FreeBSD:

- Σε ένα σύστημα που βρίσκεται ήδη σε λειτουργία, μπορείτε να εκτελέσετε το sysinstall για να εγκαταστήσετε, να διαγράψετε, και να δείτε τις εγκατεστημένες και τις διαθέσιμες εφαρμογές. Για περισσότερες πληροφορίες, δείτε το Εγκατάσταση Πακέτων.
- Τα διάφορα εργαλεία διαχείρισης μέσω της γραμμής εντολών, που αποτελούν και το αντικείμενο συζήτησης αυτής της ενότητας.

6.4.1. Εγκαθιστώντας ένα Πακέτο

Μπορείτε να χρησιμοποιήσετε το εργαλείο pkg_add(1) για να εγκαταστήσετε ένα πακέτο λογισμικού του FreeBSD από ένα τοπικά αποθηκευμένο αρχείο ή από έναν διακομιστή στο δίκτυο.

Παράδειγμα 6. "Κατέβασμα" ενός πακέτου χειροκίνητα και εγκατάσταση του τοπικά

```
# ftp -a ftp2.FreeBSD.org
Connected to ftp2.FreeBSD.org.
220 ftp2.FreeBSD.org FTP server (Version 6.00LS) ready.
331 Guest login ok, send your email address as password.
230-
230-     This machine is in Vienna, VA, USA, hosted by Verio.
230-         Questions? E-mail freebsd@vienna.verio.net.
230-
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /pub/FreeBSD/ports/packages/sysutils/
250 CWD command successful.
ftp> get lsof-4.56.4.tgz
local: lsof-4.56.4.tgz remote: lsof-4.56.4.tgz
```

```
200 PORT command successful.
150 Opening BINARY mode data connection for 'lsof-4.56.4.tgz' (92375 bytes).
100% |***************************************************| 92375       00:00 ETA
226 Transfer complete.
92375 bytes received in 5.60 seconds (16.11 KB/s)
ftp> exit
# pkg_add lsof-4.56.4.tgz
```

Εάν δεν έχετε μία τοπική πηγή πακέτων (όπως είναι ένα FreeBSD CD-ROM set) τότε ίσως είναι ευκολότερο να χρησιμοποιήσετε την επιλογή `-r` για το pkg_add(1). Αυτή θα κάνει το εργαλείο να καθορίσει αυτόματα τη σωστή μορφή και έκδοση και έπειτα να ανακτήσει και να εγκαταστήσει το πακέτο από ένα FTP site.

```
# pkg_add -r lsof
```

Το παραπάνω παράδειγμα θα "κατεβάσει" και θα εγκαταστήσει το σωστό πακέτο χωρίς περαιτέρω επέμβαση του χρήστη. Αν δεν θέλετε να χρησιμοποιήσετε το κύριο site διανομής πακέτων, μπορείτε να χρησιμοποιήσετε κάποιο mirror. Για το σκοπό αυτό, θα πρέπει να ρυθμίσετε σωστά την τιμή της `PACKAGESITE`, ώστε να παρακάμψετε τις προεπιλεγμένες ρυθμίσεις. Το pkg_add(1) χρησιμοποιεί το fetch(3) για να "κατεβάσει" τα αρχεία, και αυτό με τη σειρά του χρησιμοποιεί διάφορες μεταβλητές περιβάλλοντος, περιλαμβανομένων των `FTP_PASSIVE_MODE`, `FTP_PROXY`, και `FTP_PASSWORD`. Ίσως χρειαστεί να ρυθμίσετε μία ή περισσότερες από αυτές αν βρίσκεστε πίσω από ένα firewall, ή ίσως να χρειαστεί να χρησιμοποιήσετε έναν FTP/HTTP proxy. Δείτε το fetch(3) για την πλήρη λίστα των μεταβλητών. Προσέξτε ότι στο παραπάνω παράδειγμα χρησιμοποιείται το `lsof` αντί του `lsof-4.56.4`. Όταν γίνεται απομακρυσμένη λήψη, πρέπει να αφαιρεθεί ο αριθμός έκδοσης του πακέτου. Το pkg_add(1) θα "κατεβάσει" αυτόματα την τελευταία έκδοση της εφαρμογής.

Το pkg_add(1) θα "κατεβάσει" την τελευταία έκδοση της εφαρμογής αν χρησιμοποιείτε FreeBSD-CURRENT ή FreeBSD-STABLE. Αν τρέχετε μια -RELEASE έκδοση, θα "κατεβάσει" την έκδοση του πακέτου που έχει μεταγλωττιστεί με την έκδοση σας. Είναι δυνατό να το αλλάξετε αυτό, αλλάζοντας την `PACKAGESITE`. Για παράδειγμα, αν τρέχετε ένα σύστημα FreeBSD 8.1-RELEASE, το pkg_add(1), από προεπιλογή, θα προσπαθήσει να "κατεβάσει" πακέτα από το `ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-8.1-release/Latest/`. Αν θέλετε να αναγκάσετε το pkg_add(1) να "κατεβάσει" πακέτα του FreeBSD 8-STABLE, θέστε την `PACKAGESITE` ως `ftp://ftp.freebsd.org/pub/FreeBSD/ports/i386/packages-8-stable/Latest/`.

Τα αρχεία των πακέτων διανέμονται σε μορφές .tgz και .tbz. Μπορείτε να τα βρείτε στο ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/packages/, ή στα CD-ROM της διανομής του FreeBSD. Κάθε CD στο FreeBSD 4-CD set (και στο PowerPak, κλπ.) περιέχει πακέτα στον κατάλογο /packages. Η κατηγοριοποίηση των πακέτων ακολουθεί την δομή του δέντρου /usr/ports. Κάθε κατηγορία έχει το δικό της κατάλογο, και κάθε πακέτο μπορεί να βρεθεί στον κατάλογο All.

Η δομή των καταλόγων του συστήματος πακέτων ταιριάζει με την αντίστοιχη των ports. Τα δύο συστήματα συνεργάζονται μεταξύ τους για να δημιουργήσουν το συνολικό σύστημα πακέτων/ports.

6.4.2. Διαχείριση των Πακέτων

Το pkg_info(1) είναι ένα εργαλείο που παραθέτει και περιγράφει τα διάφορα πακέτα που είναι εγκαταστημένα.

```
# pkg_info
cvsup-16.1          A general network file distribution system optimized for CV
docbook-1.2         Meta-port for the different versions of the DocBook DTD
...
```

Το pkg_version(1) είναι ένα εργαλείο που συνοψίζει τις εκδόσεις όλων των εγκαταστημένων πακέτων. Συγκρίνει την έκδοση κάθε πακέτου, με την τρέχουσα έκδοση που βρίσκεται στο δέντρο των ports.

```
# pkg_version
cvsup                       =
docbook                     =
...
```

Τα σύμβολα στην δεύτερη στήλη δηλώνουν την σχετική ηλικία μεταξύ των εγκατεστημένων εκδόσεων και των εκδόσεων που είναι διαθέσιμες στο τοπικό δέντρο των ports.

Σύμβολο	Σημασία
=	Η έκδοση του εγκατεστημένου πακέτου ταιριάζει με αυτή που είναι διαθέσιμη στο τοπικό δέντρο των ports.
<	Η εγκατεστημένη έκδοση είναι παλαιότερη από αυτή που είναι διαθέσιμη στο δέντρο των ports.
>	Η εγκατεστημένη έκδοση είναι νεότερη από αυτή που είναι διαθέσιμη στο τοπικό δέντρο των ports. (Το τοπικό δέντρο των ports είναι πιθανότατα απαρχαιωμένο.)
?	Το εγκατεστημένο πακέτο δεν βρίσκεται στα περιεχόμενα των ports. (Αυτό μπορεί να συμβεί, για παράδειγμα, αν ένα εγκατεστημένο port έχει αφαιρεθεί από την Συλλογή των Ports, ή έχει μετονομαστεί.)
*	Υπάρχουν πολλαπλές εκδόσεις του πακέτου.
!	Το εγκατεστημένο πακέτο υπάρχει στο index, αλλά για κάποιο λόγο το `pkg_version` δεν κατάφερε να συγκρίνει την έκδοση του εγκατεστημένου πακέτου με την αντίστοιχη καταχώρηση στο index.

6.4.3. Αφαιρώντας ένα Πακέτο

Για να αφαιρέσετε ένα εγκατεστημένο πακέτο λογισμικού, χρησιμοποιήστε το εργαλείο pkg_delete(1).

```
# pkg_delete xchat-1.7.1
```

Σημειώστε ότι το pkg_delete(1) απαιτεί το πλήρες όνομα και αριθμό έκδοσης του πακέτου. Η παραπάνω εντολή δεν θα λειτουργήσει αν δώσετε απλώς *xchat* αντί για *xchat-1.7.1*. Είναι ωστόσο εύκολο να χρησιμοποιήσετε την pkg_version(1) για να βρείτε την έκδοση του εγκατεστημένου πακέτου. Αντί για αυτό, μπορείτε επίσης να χρησιμοποιήσετε ένα μπαλαντέρ:

```
# pkg_delete xchat\*
```

Στην περίπτωση αυτή, θα διαγραφούν όλα τα πακέτα που τα ονόματα τους αρχίζουν με `xchat`.

6.4.4. Διάφορα

Όλες οι πληροφορίες για τα πακέτα είναι αποθηκευμένες στον κατάλογο /var/db/pkg. Στα αρχεία αυτού του καταλόγου, θα βρείτε τη περιγραφή κάθε πακέτου, καθώς και τη λίστα των αρχείων που εγκαθιστά.

6.5. Χρησιμοποιώντας την Συλλογή των Ports

Τα παρακάτω τμήματα δίνουν βασικές οδηγίες χρήσης της Συλλογής των Ports για εγκατάσταση ή διαγραφή προγραμμάτων στο σύστημα σας. Μπορείτε να βρείτε λεπτομερή περιγραφή των διαθέσιμων επιλογών του `make` και των μεταβλητών περιβάλλοντος στο ports(7).

6.5.1. Ανακτώντας την Συλλογή των Ports

Πριν μπορέσετε να εγκαταστήσετε προγράμματα μέσω των ports, πρέπει πρώτα να ανακτήσετε την Συλλογή των Ports. Πρόκειται ουσιαστικά για μια συλλογή από Makefiles, patches, και αρχεία περιγραφής που τοποθετούνται στο /usr/ports.

Όταν εγκαταστήσατε το FreeBSD σύστημα σας, το sysinstall σας ρώτησε αν θέλατε να εγκαταστήσετε την Συλλογή των Ports. Αν επιλέξατε όχι, μπορείτε να ακολουθήσετε αυτές τις οδηγίες για να ανακτήσετε την Συλλογή των Ports:

Procedure: Μέθοδος CVSup

Αυτή είναι μια γρήγορη μέθοδος για να ανακτήσετε και να διατηρήσετε ένα ανανεωμένο αντίγραφο της Συλλογής των Ports, χρησιμοποιώντας το πρωτόκολλο CVSup. Αν θέλετε να μάθετε περισσότερα για το CVSup, δείτε το Χρησιμοποιώντας το CVSup.

> Η υλοποίηση του CVSup που περιλαμβάνεται σε ένα σύστημα FreeBSD, ονομάζεται csup.

Σιγουρευθείτε ότι το /usr/ports είναι άδειο πριν εκτελέσετε το csup για πρώτη φορά! Εάν έχετε ήδη ανακτήσει τη Συλλογή των Ports μέσω κάποιας άλλης πηγής, το csup δεν θα διαγράψει patches που έχουν αφαιρεθεί στο μεταξύ.

1. Εκτελέστε το `csup`:

```
# csup -L 2 -h cvsup.FreeBSD.org /usr/shared/examples/cvsup/ports-supfile
```

Αλλάξτε το *cvsup.FreeBSD.org* με έναν κοντινό σας διακομιστή CVSup. Δείτε το CVSup Mirrors (Τοποθεσίες CVSup) για την πλήρη λίστα των mirror sites.

Αν θέλετε, μπορείτε να χρησιμοποιήσετε το δικό σας ports-supfile, ώστε να αποφύγετε (για παράδειγμα) να δηλώσετε τον διακομιστή CVSup στην γραμμή εντολών.

a. Σε αυτή την περίπτωση, ως `root`, αντιγράψτε το /usr/shared/examples/cvsup/ports-supfile σε μία νέα τοποθεσία, όπως το /root ή τον δικό σας home κατάλογο.
b. Τροποποιήστε το ports-supfile.
c. Αλλάξτε το *CHANGE_THIS.FreeBSD.org* με έναν κοντινό σας διακομιστή CVSup.Δείτε το CVSup Mirrors (Τοποθεσίες CVSup) για την πλήρη λίστα των mirror sites.
d. Εκτελέστε τώρα το `csup`, με τον ακόλουθο τρόπο:

```
# csup -L 2 /root/ports-supfile
```

2. Εκτελώντας την εντολή csup(1) αργότερα, θα "κατεβάσει" και θα εφαρμόσει όλες τις πρόσφατες αλλαγές στην Συλλογή των Ports, εκτός από το να επανα-μεταγλωττίσει τα ports για το σύστημα σας.

Procedure: Μέθοδος Portsnap

Το Portsnap είναι ένα εναλλακτικό σύστημα για την διανομή της Συλλογής των Ports. Παρακαλώ ελέγξτε το Χρησιμοποιώντας το Portsnap για μία λεπτομερή περιγραφή όλων των χαρακτηριστικών της εφαρμογής.

1. "Κατεβάστε" ένα συμπιεσμένο snapshot της Συλλογής των Ports /var/db/portsnap. Αν θέλετε, μπορείτε να αποσυνδεθείτε από το Διαδίκτυο μετά από αυτό το βήμα.

```
# portsnap fetch
```

2. Αν εκτελείτε το Portsnap για πρώτη φορά, κάντε εξαγωγή του snapshot μέσα στο /usr/ports:

```
# portsnap extract
```

Εάν ήδη έχετε ένα γεμάτο /usr/ports και απλώς το ανανεώνετε, εκτελέστε την ακόλουθη εντολή:

```
# portsnap update
```

Procedure: Μέθοδος Sysinstall

Αυτή η μέθοδος χρησιμοποιεί το sysinstall για την εγκατάσταση της Συλλογής των Ports από το μέσο εγκατάστασης. Σημειώστε ότι με αυτό τον τρόπο θα εγκαταστήσετε το παλαιό αντίγραφο της Συλλογής των Ports, που αντιστοιχεί στην ημερομηνία της έκδοσης του FreeBSD που χρησιμοποιείτε. Εάν έχετε πρόσβαση στο Διαδίκτυο, πρέπει πάντα να χρησιμοποιείτε μία από τις μεθόδους που αναφέρθηκαν πιο πάνω.

1. Ως `root`, εκτελέστε το `sysinstall` όπως φαίνεται παρακάτω:

```
# sysinstall
```

2. Επιλέξτε το Configure, και πιέστε `Enter`.
3. Επιλέξτε το Distributions, και πιέστε `Enter`.
4. Μετακινηθείτε στο ports, και πιέστε `Space`.
5. Μετακινηθείτε στο Exit, και πιέστε `Enter`.
6. Επιλέξτε το μέσο εγκατάστασης της επιθυμίας σας, όπως CDROM, FTP, και πάει λέγοντας.
7. Μετακινηθείτε στο Exit και πιέστε `Enter`.
8. Πιέστε `X` για να βγείτε από το sysinstall.

6.5.2. Εγκαθιστώντας Ports

Το πρώτο πράγμα που πρέπει να διευκρινιστεί σχετικά με την Συλλογή των Ports είναι η έννοια του όρου "skeleton (σκελετός)". Με λίγα λόγια, ένα port skeleton είναι η ελάχιστη συλλογή αρχείων που καθοδηγούν ένα σύστημα FreeBSD ώστε να μεταγλωττίσει και να εγκαταστήσει σωστά ένα πρόγραμμα. Κάθε port skeleton περιέχει:

- Ένα Makefile. Το Makefile περιέχει διάφορες δηλώσεις που ορίζουν πως πρέπει να μεταγλωττιστεί η εφαρμογή και που πρέπει να εγκατασταθεί στο σύστημά σας.
- Ένα αρχείο distinfo. Αυτό το αρχείο περιέχει πληροφορίες για τα αρχεία που πρέπει να "κατέβουν" για την μεταγλώττιση του port, και τα checksums τους (χρησιμοποιώντας το sha256(1)), για να επιβεβαιωθεί ότι τα αρχεία δεν έχουν αλλοιωθεί κατά την διάρκεια της μεταφοράς τους.
- Έναν κατάλογο files. Αυτός ο κατάλογος περιέχει τα patches που επιτρέπουν στο πρόγραμμα να μεταγλωττιστεί και εγκατασταθεί στο FreeBSD σύστημα σας. Τα patches είναι μικρά αρχεία που ορίζουν αλλαγές σε συγκεκριμένα αρχεία. Είναι σε μορφή κοινού κειμένου, και βασικά λένε

"Αφαίρεσε την γραμμή 10" ή "Μετέτρεψε τη γραμμή 26 σε αυτό ...". Τα patches είναι επίσης γνωστά ως "diffs" επειδή δημιουργούνται με το πρόγραμμα diff(1).

Αυτός ο κατάλογος μπορεί να περιέχει και άλλα αρχεία που χρησιμοποιούνται για να μεταγλωττιστεί το port.

- Ένα αρχείο pkg-descr. Αυτό είναι μία πιο λεπτομερής, συχνά πολλών γραμμών, περιγραφή του προγράμματος.
- Ένα αρχείο pkg-plist. Αυτό περιέχει μια λίστα όλων των αρχείων που θα εγκατασταθούν από το port. Επίσης καθοδηγεί το σύστημα των ports τι αρχεία να αφαιρέσει κατά την απεγκατάσταση.

Μερικά ports έχουν και άλλα αρχεία, όπως το pkg-message. Το σύστημα των ports χρησιμοποιεί αυτά τα αρχεία για να χειριστεί ειδικές περιστάσεις. Αν θέλετε περισσότερες λεπτομέρειες για αυτά τα αρχεία, και τα ports γενικότερα, δείτε το FreeBSD Porter's Handbook.

Το port περιέχει οδηγίες για το πως να μεταγλωττιστεί ο πηγαίος κώδικας, αλλά δεν περιέχει τον πηγαίο κώδικα. Μπορείτε να προμηθευτείτε τον πηγαίο κώδικα από ένα CD-ROM ή από το Διαδίκτυο. Ο πηγαίος κώδικας διανέμεται με οποιοδήποτε τρόπο επιθυμεί ο δημιουργός του. Συχνά είναι ένα tarred και gzipped αρχείο, αλλά μπορεί να είναι συμπιεσμένος με κάποιο άλλο εργαλείο ή να είναι ακόμα και ασυμπίεστος. Ο πηγαίος κώδικας του προγράμματος, σε οποιαδήποτε μορφή κι αν διατίθεται, λέγεται "distfile". Οι δύο μέθοδοι για να εγκαταστήσετε ένα FreeBSD port περιγράφονται παρακάτω.

Πρέπει να συνδεθείτε ως `root` για να εγκαταστήσετε ports.

Πριν εγκαταστήσετε οποιαδήποτε port, πρέπει να σιγουρευτείτε ότι έχετε μία ανανεωμένη Συλλογή των Ports, και πρέπει να ελέγξετε το http://vuxml.freebsd.org/ για θέματα ασφαλείας σχετικά με το port που ενδιαφέρεστε.

Αν θέλετε να ελέγχετε αυτόματα για τυχόν προβλήματα ασφαλείας πριν από κάθε εγκατάσταση νέας εφαρμογής, μπορείτε να χρησιμοποιήσετε το portaudit. Θα βρείτε αυτό το εργαλείο στην Συλλογή των Ports (ports-mgmt/portaudit). Είναι καλή ιδέα να εκτελέσετε το `portaudit -F` πριν εγκαταστήσετε ένα νέο port, για να ανακτήσετε την τρέχουσα βάση δεδομένων προβλημάτων ασφαλείας. Αντίστοιχος έλεγχος και ανανέωση της βάσης δεδομένων εκτελείται επίσης αυτόματα κατά τον καθημερινό έλεγχο ασφαλείας του συστήματος. Για περισσότερες πληροφορίες διαβάστε τις σελίδες manual portaudit(1) και periodic(8).

Η Συλλογή των Ports προϋποθέτει ότι έχετε λειτουργική σύνδεση με το Διαδίκτυο. Εάν δεν έχετε, θα χρειαστεί να βάλετε μόνος σας ένα αντίγραφο του distfile μέσα στο /usr/ports/distfiles.

Αρχικά, μετακινηθείτε στον κατάλογο του port που θέλετε να εγκαταστήσετε:

```
# cd /usr/ports/sysutils/lsof
```

Μόλις βρεθείτε στον κατάλογο lsof, θα δείτε τον port skeleton. Το επόμενο βήμα είναι να

μεταγλωττίσετε, ή να "κτίσετε (build)", το port. Αυτό γίνεται απλά πληκτρολογώντας `make` στην γραμμή εντολών. Όταν το κάνετε, θα δείτε κάτι όπως αυτό:

```
# make
>> lsof_4.57D.freebsd.tar.gz doesn't seem to exist in /usr/ports/distfiles/.
>> Attempting to fetch from ftp://lsof.itap.purdue.edu/pub/tools/unix/lsof/.
===>  Extracting for lsof-4.57
...
[extraction output snipped]
...
>> Checksum OK for lsof_4.57D.freebsd.tar.gz.
===>  Patching for lsof-4.57
===>  Applying FreeBSD patches for lsof-4.57
===>  Configuring for lsof-4.57
...
[configure output snipped]
...
===>  Building for lsof-4.57
...
[compilation output snipped]
...
#
```

Προσέξτε ότι μόλις η μεταγλώττιση ολοκληρωθεί θα επιστρέψετε στην γραμμή εντολών. Το επόμενο βήμα είναι να εγκαταστήσετε το port. Για να το εγκαταστήσετε, χρειάζεται απλώς να προσθέσετε μια λέξη στην εντολή `make`, και αυτή η λέξη είναι `install`:

```
# make install
===>  Installing for lsof-4.57
...
[installation output snipped]
...
===>   Generating temporary packing list
===>   Compressing manual pages for lsof-4.57
===>   Registering installation for lsof-4.57
===>  SECURITY NOTE:
      This port has installed the following binaries which execute with
      increased privileges.
#
```

Μόλις επιστρέψετε στην γραμμή εντολών, θα πρέπει να μπορείτε να εκτελέσετε την εφαρμογή που μόλις εγκαταστήσατε. Θα δείτε μια προειδοποίηση ασφαλείας, επειδή το `lsof` είναι ένα πρόγραμμα που τρέχει με αυξημένα προνόμια. Κατά την μεταγλώττιση και εγκατάσταση των ports, θα πρέπει να προσέχετε οποιαδήποτε προειδοποίηση εμφανιστεί.

Μια καλή ιδέα, είναι να διαγράψετε τον υποκατάλογο που περιέχει όλα τα προσωρινά αρχεία που χρησιμοποιήθηκαν κατά την μεταγλώττιση. Όχι μόνο καταναλώνουν πολύτιμο χώρο, άλλα μπορεί να προκαλέσουν προβλήματα αργότερα όταν θα θελήσετε να εγκαταστήσετε μια νεότερη έκδοση του

port.

```
# make clean
===>  Cleaning for lsof-4.57
#
```

Μπορείτε να γλιτώσετε δύο πρόσθετα βήματα απλώς εκτελώντας `make install clean` αντί για `make`, `make install` και `make clean` ως τρία ξεχωριστά βήματα.

Μερικά κελύφη κρατάνε μια λίστα από τις εντολές που βρίσκονται διαθέσιμες στους καταλόγους που αναφέρονται στην μεταβλητή περιβάλλοντος `PATH`, για να επιταχύνουν τις αναζητήσεις για τα εκτελέσιμα αρχεία αυτών των εντολών. Αν χρησιμοποιείτε ένα από αυτά τα κελύφη, θα πρέπει να χρησιμοποιήσετε την εντολή `rehash` μετά την εγκατάσταση ενός port, πριν μπορέσετε να χρησιμοποιήσετε τις νέες εντολές. Αυτή η εντολή λειτουργεί σε κελύφη όπως το `tcsh`. Χρησιμοποιήστε την εντολή `hash -r` για κελύφη όπως το `sh`. Δείτε την τεκμηρίωση του κελύφους σας για περισσότερες πληροφορίες.

Μερικά προϊόντα τρίτων κατασκευαστών σε DVD-ROM, όπως το FreeBSD Toolkit από το FreeBSD Mall, περιέχουν distfiles. Αυτά μπορούν να χρησιμοποιηθούν με την Συλλογή των Ports. Προσαρτήστε το DVD-ROM στο /cdrom. Αν χρησιμοποιείτε κάποιο διαφορετικό σημείο προσάρτησης, ρυθμίστε την μεταβλητή `CD_MOUNTPTS` του make. Τα αναγκαία distfiles θα χρησιμοποιηθούν αυτόματα αν υπάρχουν στο δισκάκι.

Πρέπει να γνωρίζετε ότι οι άδειες μερικών ports δεν επιτρέπουν την διανομή τους σε CD-ROM. Αυτό μπορεί να οφείλεται π.χ. στο ότι πρέπει να συμπληρώσετε μια φόρμα εγγραφής πριν "κατεβάσετε" την εφαρμογή, ή στο ότι δεν επιτρέπεται η επαναδιανομή, ή σε κάποιο άλλο λόγο. Εάν θέλετε να εγκαταστήσετε ένα port που δεν περιλαμβάνεται στο CD-ROM, θα χρειαστεί να είστε συνδεδεμένος στο Διαδίκτυο για να το επιτύχετε.

Το σύστημα των ports χρησιμοποιεί το fetch(3) για να "κατεβάσει" τα αρχεία. Το fetch(3) χρησιμοποιεί διάφορες μεταβλητές περιβάλλοντος, περιλαμβανομένων των `FTP_PASSIVE_MODE`, `FTP_PROXY`, και `FTP_PASSWORD`. Ίσως χρειαστεί να ρυθμίσετε μία ή περισσότερες αν βρίσκεστε πίσω από ένα firewall, ή ίσως να χρειαστεί να χρησιμοποιήσετε έναν FTP/HTTP proxy. Δείτε το fetch(3) για μια πλήρη λίστα των μεταβλητών αυτών.

Για χρήστες που δεν μπορούν να είναι συνδεδεμένοι όλη την ώρα, διατίθεται η επιλογή `make fetch`. Απλώς εκτελέστε την εντολή στον κατάλογο (/usr/ports) και τα απαραίτητα αρχεία θα "κατέβουν" για εσάς. Η εντολή αυτή θα λειτουργήσει και σε υποκαταλόγους, όπως για παράδειγμα: /usr/ports/net. Προσέξτε ότι αν ένα port εξαρτάται από βιβλιοθήκες ή άλλα ports, η εντολή αυτή *δεν* θα ανακτήσει τα distfiles τους. Αντικαταστήστε το `fetch` με το `fetch-recursive` αν θέλετε μαζί με το port να ανακτήσετε και όλες τις εξαρτήσεις του.

Μπορείτε να μεταγλωττίσετε όλα τα ports σε μία κατηγορία ή ακόμα και σε όλες, εκτελώντας το `make` στον αρχικό κατάλογο, όπως με την προαναφερθείσα `make fetch` μέθοδο. Αυτό όμως είναι επικίνδυνο, γιατί μερικά ports δεν μπορούν να

συνυπάρχουν. Σε άλλες περιπτώσεις, μερικά ports μπορεί να εγκαταστήσουν δυο διαφορετικά αρχεία με το με το ίδιο όνομα.

Σε μερικές σπάνιες περιπτώσεις, οι χρήστες μπορεί να χρειάζεται να ανακτήσουν τα tarballs από ένα site διαφορετικό από τα MASTER_SITES (η τοποθεσία από όπου "κατεβαίνουν" τα αρχεία). Μπορείτε να αλλάξετε την επιλογή MASTER_SITES με την ακόλουθη εντολή:

```
# cd /usr/ports/directory
# make MASTER_SITE_OVERRIDE= \
ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/ fetch
```

Σε αυτό το παράδειγμα αλλάξαμε την επιλογή MASTER_SITES σε ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/.

Μερικά ports επιτρέπουν (ή απαιτούν) να δώσετε επιλογές μεταγλώττισης που μπορούν να ενεργοποιήσουν/απενεργοποιήσουν τμήματα της εφαρμογής που είναι αχρείαστα, συγκεκριμένες επιλογές ασφαλείας, και άλλες τροποποιήσεις. Κοινά παραδείγματα τέτοιων ports είναι τα www/firefox, security/gpgme, και το mail/sylpheed-claws. Όταν υπάρχουν διαθέσιμες τέτοιες επιλογές, θα εμφανιστεί στην οθόνη σας σχετικό μήνυμα.

6.5.2.1. Παρακάμπτοντας τους Προεπιλεγμένους Καταλόγους των Ports

Μερικές φορές είναι χρήσιμο (ή επιτακτικό) να χρησιμοποιήσετε ένα διαφορετικό κατάλογο εργασίας και εγκατάστασης. Οι μεταβλητές WRKDIRPREFIX και PREFIX μπορούν να παρακάμψουν τους προεπιλεγμένους καταλόγους. Για παράδειγμα, η εντολή:

```
# make WRKDIRPREFIX=/usr/home/example/ports install
```

θα μεταγλωττίσει το port στο /usr/home/example/ports και θα εγκαταστήσει τα πάντα στο /usr/local, ενώ η εντολή:

```
# make PREFIX=/usr/home/example/local install
```

θα μεταγλωττίσει το port στο /usr/ports και θα το εγκαταστήσει στο /usr/home/example/local.

Και φυσικά η εντολή:

```
# make WRKDIRPREFIX=../ports PREFIX=../local install
```

θα συνδυάσει και τα δυο (είναι πολύ μεγάλη για να την δείξουμε εδώ, άλλα πρέπει να πήρατε την γενική ιδέα).

Εναλλακτικά, αυτές οι μεταβλητές μπορούν να ρυθμιστούν ως μέρος του περιβάλλοντος σας. Διαβάστε την σελίδα manual για το κέλυφος σας, για να βρείτε τις σχετικές οδηγίες.

6.5.2.2. Αντιμετωπίζοντας το `imake`

Μερικά ports που χρησιμοποιούν το `imake` (μέρος του X Window System) δεν συνεργάζονται σωστά με το `PREFIX`, και επιμένουν να εγκατασταθούν στο /usr/X11R6. Όμοια, μερικά Perl ports αγνοούν το `PREFIX` και εγκαθίστανται στο δέντρο Perl. Το να κάνετε αυτά τα ports να σέβονται το `PREFIX` είναι μία δύσκολη ή αδύνατη δουλειά.

6.5.2.3. Επαναρύθμιση Επιλογών Ports

Όταν μεταγλωττίζετε κάποια ports, μπορεί να εμφανιστεί στην οθόνη σας ένα μενού επιλογών (βασισμένο σε ncurses) το οποίο να σας επιτρέπει να αλλάξετε διάφορες επιλογές μεταγλώττισης. Δεν είναι σπάνιο κάποιοι χρήστες να θέλουν να επισκεφτούν ξανά αυτό το μενού, για να προσθέσουν, να αφαιρέσουν ή να αλλάξουν κάποιες επιλογές, μετά την μεταγλώττιση του port. Μια επιλογή είναι να μετακινηθείτε στον κατάλογο του port και να γράψετε `make config`, με το οποίο θα εμφανιστεί ξανά το μενού με τις προηγούμενες ρυθμίσεις σας ήδη επιλεγμένες. Μια άλλη δυνατότητα, είναι να χρησιμοποιήσετε την εντολή `make showconfig`, με την οποία θα δείτε όλες τις επιλεγμένες ρυθμίσεις του port. Τέλος, μια ακόμα επιλογή είναι να εκτελέσετε την εντολή `make rmconfig` η οποία θα αφαιρέσει όλες τις αποθηκευμένες επιλογές και θα σας επιτρέψει να ξεκινήσετε ξανά από την αρχή. Όλες αυτές οι επιλογές, και ακόμα περισσότερες, εξηγούνται στη σελίδα manual του ports(7).

6.5.3. Αφαιρώντας Εγκατεστημένα Ports

Τώρα που γνωρίσατε πως να εγκαθιστάτε ports, πιθανώς θα αναρωτιέστε πως αφαιρούνται, στην περίπτωση που εγκαταστήσατε ένα και αργότερα αποφασίσατε ότι εγκαταστήσατε το λάθος port. Θα αφαιρέσουμε το προηγούμενο παράδειγμα (που ήταν το `lsof` για όσους δεν το πρόσεξαν). Τα ports αφαιρούνται όπως και τα πακέτα (το αναλύσαμε στην ενότητα Χρησιμοποιώντας το Σύστημα των Πακέτων), χρησιμοποιώντας την εντολή pkg_delete(1):

```
# pkg_delete lsof-4.57
```

6.5.4. Αναβαθμίζοντας τα Ports

Αρχικά, δείτε τα παρωχημένα ports για τα οποία υπάρχουν διαθέσιμες νεότερες εκδόσεις στην Συλλογή των Ports, με την εντολή pkg_version(1):

```
# pkg_version -v
```

6.5.4.1. /usr/ports/UPDATING

Μόλις ανανεώσετε την Συλλογή των Ports, πρέπει να ελέγξετε το αρχείο /usr/ports/UPDATING, πριν επιχειρήσετε την αναβάθμιση ενός port. Αυτό το αρχείο περιγράφει διάφορα πιθανά προβλήματα, καθώς και ενδεχόμενα πρόσθετα βήματα που πρέπει να εκτελέσετε όταν ανανεώνετε ένα port. Παραδείγματα των παραπάνω, είναι η αλλαγή μορφής κάποιων αρχείων, αλλαγή στην τοποθεσία των αρχείων ρυθμίσεων, ή άλλες ασυμβατότητες με παλαιότερες εκδόσεις.

Αν το UPDATING αναιρεί κάτι που διαβάσατε εδώ, θεωρήστε ότι ισχύει το UPDATING.

6.5.4.2. Αναβαθμίζοντας Ports με το Portupgrade

Το εργαλείο portupgrade είναι σχεδιασμένο για να αναβαθμίζει εύκολα εγκατεστημένα ports. Διατίθεται από το ports-mgmt/portupgrade port. Εγκαταστήστε το όπως κάθε port, χρησιμοποιώντας την εντολή `make install clean`:

```
# cd /usr/ports/ports-mgmt/portupgrade
# make install clean
```

Η εντολή `pkgdb -F` θα διαβάσει και θα διορθώσει όλες τις ασυνέπειες που ίσως υπάρχουν στη λίστα των εγκατεστημένων ports. Είναι καλή ιδέα είναι να την εκτελείτε συχνά, ενδεχομένως πριν από κάθε αναβάθμιση.

Όταν εκτελείτε το `portupgrade -a`, το portupgrade θα αρχίσει να αναβαθμίζει όλα τα παρωχημένα ports που είναι εγκατεστημένα στο σύστημα σας. Χρησιμοποιήστε την επιλογή `-i` αν θέλετε να σας ρωτά για επιβεβαίωση για κάθε ξεχωριστή αναβάθμιση.

```
# portupgrade -ai
```

Αν θέλετε να αναβαθμίσετε μόνο μία συγκεκριμένη εφαρμογή, και όχι όλα τα διαθέσιμα ports, χρησιμοποιήστε το `portupgrade pkgname`. Συμπεριλάβετε την επιλογή `-R` αν το portupgrade πρέπει πρώτα να αναβαθμίσει όλα τα ports που απαιτούνται για την συγκεκριμένη εφαρμογή.

```
# portupgrade -R firefox
```

Για να χρησιμοποιήσετε πακέτα αντί για ports στην εγκατάσταση, δώστε την επιλογή `-P`. Με αυτή την επιλογή το portupgrade αναζητά τους τοπικούς καταλόγους που ορίζονται στο `PKG_PATH`, ή ανακτά τα πακέτα από απομακρυσμένα sites εάν δεν βρεθούν τοπικά. Αν τα πακέτα δεν μπορούν να ανακτηθούν με τους παραπάνω τρόπους, το portupgrade θα χρησιμοποιήσει τα ports. Για να αποφύγετε εντελώς την χρήση των ports, καθορίστε την επιλογή `-PP`.

```
# portupgrade -PR gnome2
```

Για να ανακτήσετε απλώς τα distfiles (ή τα πακέτα, αν έχετε ορίσει την επιλογή `-P`) χωρίς να μεταγλωττίσετε ή να εγκαταστήσετε τίποτα, χρησιμοποιήστε το `-F`. Για περισσότερες πληροφορίες, δείτε το portupgrade(1).

6.5.4.3. Αναβαθμίζοντας Ports με το Portmanager

Το Portmanager είναι ένα ακόμα εργαλείο για εύκολη αναβάθμιση εγκατεστημένων ports. Διατίθεται από το ports-mgmt/portmanager port:

```
# cd /usr/ports/ports-mgmt/portmanager
# make install clean
```

Όλα τα εγκατεστημένα ports μπορούν να αναβαθμιστούν χρησιμοποιώντας αυτή την απλή εντολή:

```
# portmanager -u
```

Μπορείτε να προσθέσετε την επιλογή `-ui` στην παραπάνω εντολή (`portmanager -u -ui`) για να ερωτηθείτε να επιβεβαιώσετε κάθε βήμα που θα εκτελέσει το Portmanager. Το Portmanager μπορεί επίσης να χρησιμοποιηθεί για να εγκαταστήσετε νέα ports στο σύστημα. Σε αντίθεση με την εντολή `make install clean`, το Portmanager θα αναβαθμίσει όλες τις εξαρτήσεις πριν την μεταγλώττιση και εγκατάσταση του επιλεγμένου port.

```
# portmanager x11/gnome2
```

Αν υπάρχουν προβλήματα που σχετίζονται με τις εξαρτήσεις ενός επιλεγμένου port, μπορείτε να χρησιμοποιήσετε το Portmanager για να τις επανα-μεταγλωττίσει όλες με την σωστή σειρά. Μόλις τελειώσει με τις εξαρτήσεις, θα επανα-μεταγλωττίσει και το προβληματικό port.

```
# portmanager graphics/gimp -f
```

Για περισσότερες πληροφορίες δείτε τη σελίδα manual portmanager(1).

6.5.4.4. Αναβαθμίζοντας τα Ports μέσω του Portmaster

Το Portmaster είναι ένα ακόμα εργαλείο για την αναβάθμιση των εγκατεστημένων ports. Το Portmaster σχεδιάστηκε ώστε να χρησιμοποιεί τα εργαλεία που παρέχει το "βασικό" σύστημα (δεν εξαρτάται από άλλα ports) και χρησιμοποιεί τις πληροφορίες του /var/db/pkg για να καθορίσει ποια ports θα αναβαθμίσει. Είναι διαθέσιμο μέσω του port ports-mgmt/portmaster:

```
# cd /usr/ports/ports-mgmt/portmaster
# make install clean
```

Το Portmaster ομαδοποιεί τα ports σε τέσσερις κατηγορίες:

- Root ports (δεν εξαρτώνται από άλλα, και ούτε άλλα εξαρτώνται από αυτά)
- Trunk ports (δεν εξαρτώνται από άλλα, ωστόσο κάποια πακέτα εξαρτώνται από αυτά)
- Branch ports (έχουν εξαρτήσεις και προς τις δύο κατευθύνσεις)
- Leaf ports (εξαρτώνται από άλλα, αλλά όχι το αντίθετο)

Μπορείτε να δείτε μια λίστα όλων των εγκατεστημένων ports και να ψάξετε για ενημερωμένες εκδόσεις, χρησιμοποιώντας την επιλογή `-L`:

```
# portmaster -L
===>>> Root ports (No dependencies, not depended on)
===>>> ispell-3.2.06_18
===>>> screen-4.0.3
```

```
        ===>>> New version available: screen-4.0.3_1
===>>> tcpflow-0.21_1
===>>> 7 root ports
...
===>>> Branch ports (Have dependencies, are depended on)
===>>> apache-2.2.3
        ===>>> New version available: apache-2.2.8
...
===>>> Leaf ports (Have dependencies, not depended on)
===>>> automake-1.9.6_2
===>>> bash-3.1.17
        ===>>> New version available: bash-3.2.33
...
===>>> 32 leaf ports

===>>> 137 total installed ports
        ===>>> 83 have new versions available
```

Μπορείτε να αναβαθμίσετε όλα τα εγκατεστημένα ports με την παρακάτω απλή εντολή:

```
# portmaster -a
```

Από προεπιλογή, το Portmaster θα δημιουργήσει αντίγραφο ασφαλείας του εγκατεστημένου πακέτου πριν το διαγράψει. Αν η εγκατάσταση της νέας έκδοσης είναι επιτυχής, το Portmaster θα σβήσει το αντίγραφο αυτό. Αν χρησιμοποιήσετε την επιλογή `-b`, το Portmaster δεν θα σβήσει αυτόματα το αντίγραφο. Αν χρησιμοποιήσετε την επιλογή `-i`, θα θέσετε το Portmaster σε διαδραστική λειτουργία, όπου θα σας ζητάει επιβεβαίωση πριν την αναβάθμιση κάθε port.

Αν αντιμετωπίσετε λάθη κατά τη διαδικασία της αναβάθμισης, μπορείτε να χρησιμοποιήσετε την επιλογή `-f` για να αναβαθμίσετε και να μεταγλωττίσετε ξανά όλα τα ports:

```
# portmaster -af
```

Μπορείτε επίσης να χρησιμοποιήσετε το Portmaster για να εγκαταστήσετε νέα ports στο σύστημα σας, αναβαθμίζοντας και όλες τις εξαρτήσεις τους πριν τη μεταγλώττιση και εγκατάσταση τους:

```
# portmaster shells/bash
```

Παρακαλούμε δείτε τη σελίδα manual του portmaster(8) για περισσότερες πληροφορίες.

6.5.5. Ports και Αποθηκευτικός Χώρος

Η Συλλογή των Ports καταναλώνει διαθέσιμο χώρο στο δίσκο με την πάροδο του χρόνου. Μετά την μεταγλώττιση και εγκατάσταση λογισμικού από τα ports, πρέπει πάντα να θυμάστε να καθαρίζετε τους προσωρινούς καταλόγους work χρησιμοποιώντας την εντολή `make clean`. Μπορείτε να

καθαρίσετε όλη την Συλλογή των Ports με την ακόλουθη εντολή:

```
# portsclean -C
```

Με την πάροδο του χρόνου, θα συσσωρευτούν πολλά αρχεία διανομής πηγαίου κώδικα στον κατάλογο distfiles. Μπορείτε να τα αφαιρέσετε χειροκίνητα, ή μπορείτε να χρησιμοποιήσετε την ακόλουθη εντολή για να διαγράψετε όλα τα distfiles που δεν σχετίζονται πλέον με κανένα port:

```
# portsclean -D
```

Ή για να αφαιρέσετε όλα τα distfiles που δεν σχετίζονται με κανένα port που βρίσκεται εγκατεστημένο στο σύστημα σας:

```
# portsclean -DD
```

Το εργαλείο `portsclean` εγκαθίσταται ως μέρος του portupgrade.

Μην ξεχνάτε να αφαιρείτε τα εγκατεστημένα ports όταν δεν τα χρειάζεστε πλέον. Ένα καλό εργαλείο για να αυτοματοποιηθεί αυτή η εργασία, είναι το port ports-mgmt/pkg_cutleaves.

6.6. Ενέργειες μετά την Εγκατάσταση

Μετά την εγκατάσταση μιας νέας εφαρμογής, λογικά θα θέλετε να διαβάσετε ότι τεκμηρίωση υπάρχει, να τροποποιήσετε τα αρχεία ρυθμίσεων που χρειάζεται, να βεβαιωθείτε ότι η εφαρμογή ξεκινάει κατά την εκκίνηση (αν είναι daemon), κ.λ.π.

Τα ακριβή βήματα που θα χρειαστούν για να ρυθμίσετε κάθε εφαρμογή, θα είναι προφανώς διαφορετικά. Όμως, αν μόλις εγκαταστήσατε μια νέα εφαρμογή και αναρωτιέστε "Τώρα τι;" οι παρακάτω συμβουλές μπορεί να σας βοηθήσουν:

- Χρησιμοποιήστε το pkg_info(1) για να δείτε τι αρχεία εγκαταστάθηκαν, και που. Για παράδειγμα, αν μόλις εγκαταστήσατε το FooPackage version 1.0.0, τότε η εντολή:

  ```
  # pkg_info -L foopackage-1.0.0 | less
  ```

  θα σας δείξει όλα τα αρχεία που εγκαταστάθηκαν από αυτό το πακέτο. Προσέξτε τα αρχεία στον κατάλογο man/, που θα είναι σελίδες manual, τους κατάλογους etc/, όπου θα είναι τα αρχεία ρυθμίσεων, και το doc/, όπου θα βρίσκεται πιο περιεκτική τεκμηρίωση.

  Αν δεν είστε σίγουρος ποια έκδοση της εφαρμογής εγκαταστήσατε, μια εντολή όπως αυτή:

  ```
  # pkg_info | grep -i foopackage
  ```

θα βρει όλα τα εγκατεστημένα πακέτα που έχουν το *foopackage* στο όνομα του πακέτου. Αντικαταστήστε το *foopackage* στην γραμμή εντολών με το πακέτο που αναζητάτε.

- Μόλις δείτε που βρίσκονται τα manual pages της εφαρμογής, δείτε τα με την man(1). Όμοια, δείτε τα παραδείγματα των αρχείων ρύθμισης, και όποια άλλη πρόσθετη τεκμηρίωση διατίθεται.
- Αν υπάρχει web site για την εφαρμογή, ελέγξτε το για πρόσθετη τεκμηρίωση, συχνές ερωτήσεις (FAQ), και άλλα. Αν δεν είστε σίγουρος για την διεύθυνσή του web site, ίσως το βρείτε στην έξοδο της εντολής:

```
# pkg_info foopackage-1.0.0
```

Αν υπάρχει γραμμή `WWW:`, θα πρέπει να έχει το URL για το web site της εφαρμογής.

- Ports που πρέπει να ξεκινούν κατά την εκκίνηση (όπως διακομιστές Internet) συνήθως εγκαθιστούν ένα script στο /usr/local/etc/rc.d. Πρέπει να ελέγξετε το script για την ορθότητα του και να το τροποποιήσετε ή να το μετονομάσετε αν χρειάζεται. Δείτε το Εκκινώντας Υπηρεσίες για περισσότερες πληροφορίες.

6.7. Αντιμετωπίζοντας Χαλασμένα Ports

Αν έρθετε αντιμέτωπος με ένα port το οποίο δεν λειτουργεί, υπάρχουν κάποια πράγματα που μπορείτε να κάνετε:

1. Δείτε αν εκκρεμεί κάποια διόρθωση για το port στο Problem Report database. Εάν ναι, μπορείτε να χρησιμοποιήσετε τη προτεινόμενη διόρθωση.
2. Ζητήστε βοήθεια από τον συντηρητή του port. Πληκτρολογήστε `make maintainer` ή διαβάστε το Makefile για να βρείτε την διεύθυνση email του συντηρητή. Στο μήνυμα σας, θυμηθείτε να συμπεριλάβετε το όνομα και την έκδοση του port (στείλτε τη γραμμή `$FreeBSD:` από το Makefile) καθώς και την έξοδο του σφάλματος.

Μερικά ports δεν συντηρούνται από κάποιο συγκεκριμένο άτομο, αλλά από κάποια mailing list. Πολλές, αν όχι όλες, από αυτές τις διευθύνσεις έχουν την μορφή freebsd-listname@FreeBSD.org. Παρακαλούμε να το έχετε υπόψη σας κατά τη διατύπωση των ερωτήσεων σας.

Συγκεκριμένα, τα ports που φαίνονται ότι συντηρούνται από το ports@FreeBSD.org, δεν συντηρούνται από κανέναν στην πραγματικότητα. Διορθώσεις και υποστήριξη, αν υπάρχουν, έρχονται γενικά από την κοινότητα που συμμετέχει στην συγκεκριμένη mailing list. Χρειαζόμαστε πάντοτε περισσότερους εθελοντές!

Αν δεν λάβετε απάντηση, μπορείτε να χρησιμοποιήσετε το send-pr(1) για να στείλετε μια αναφορά σφάλματος (δείτε το Γράφοντας Αναφορές Σφάλματος για το FreeBSD).

3. Διορθώστε το! Το Porter's Handbook περιέχει λεπτομερείς πληροφορίες για την υποδομή των "Ports" ώστε να μπορείτε να διορθώσετε το περιστασιακό προβληματικό port ή ακόμα και να δημιουργήσετε ένα δικό σας port!

4. Ανακτήστε το πακέτο από ένα κοντινό σας FTP site. Η "κύρια" συλλογή πακέτων βρίσκεται στο ftp.FreeBSD.org, στον κατάλογο πακέτων. Πριν τη χρησιμοποιήσετε, ελέγξτε *πρώτα* το τοπικό σας mirror. Τα πακέτα είναι πιο σίγουρο ότι θα λειτουργήσουν, από το να προσπαθείτε να μεταγλωττίσετε τον πηγαίο κώδικα, και η διαδικασία τελειώνει πιο γρήγορα. Χρησιμοποιήστε το πρόγραμμα pkg_add(1) για να εγκαταστήσετε το πακέτο στο σύστημα σας.

Chapter 7. Το Σύστημα X Window

7.1. Σύνοψη

Το FreeBSD χρησιμοποιεί το X11 για να παρέχει στους χρήστες ένα ισχυρό γραφικό περιβάλλον εργασίας. Το περιβάλλον X11 είναι μια υλοποίηση ανοικτού κώδικα του συστήματος X Window που υλοποιείται στο Xorg (καθώς και σε άλλο λογισμικό που δεν περιγράφεται εδώ). Η προεπιλεγμένη και επίσημη διανομή του X11 είναι το Xorg, ο X11 server που αναπτύχθηκε από το X.Org Foundation με άδεια χρήσης αρκετά όμοια με αυτή που χρησιμοποιείται από το FreeBSD. Υπάρχουν επίσης διαθέσιμοι εμπορικοί X servers για το FreeBSD.

Για περισσότερες πληροφορίες που σχετίζονται με τις κάρτες γραφικών που υποστηρίζονται από το περιβάλλον X11, δείτε την δικτυακή τοποθεσία Xorg.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τα διάφορα τμήματα του συστήματος X Window, και πως συνεργάζονται μεταξύ τους.
- Πως να εγκαταστήσετε και να ρυθμίσετε το περιβάλλον X11.
- Πως να εγκαταστήσετε και να ρυθμίσετε διαφορετικούς διαχειριστές παραθύρων (window managers).
- Πως να χρησιμοποιήσετε TrueType® γραμματοσειρές στο X11.
- Πως να ρυθμίσετε το σύστημα σας για σύνδεση (login) μέσω γραφικού περιβάλλοντος (XDM).

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ξέρετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

7.2. Κατανόηση του περιβάλλοντος X11

Η χρήση του περιβάλλοντος X11 για πρώτη φορά μπορεί να προκαλέσει μια μικρή ταραχή σε όποιον έχει συνηθίσει σε άλλα γραφικά περιβάλλοντα, όπως τα Microsoft® Windows® ή το Mac OS®.

Γενικά, δεν είναι απαραίτητο να καταλαβαίνετε με κάθε λεπτομέρεια των διαφόρων τμημάτων του X11 και πώς αλληλεπιδρούν μεταξύ τους. Κάποιες βασικές γνώσεις όμως, είναι χρήσιμες και βοηθούν στο να εκμεταλλευτείτε καλύτερα τις δυνατότητες του X11.

7.2.1. Γιατί λέγεται X11 το περιβάλλον εργασίας;

Το X δεν είναι το πρώτο περιβάλλον εργασίας που γράφτηκε για συστήματα UNIX®, αλλά είναι σήμερα το πιο δημοφιλές. Η αρχική ομάδα ανάπτυξης του X είχε δουλέψει σε ένα άλλο σύστημα πριν γράψει το X. Το όνομα του παλιότερου συστήματος ήταν "W" (από την Αγγλική λέξη "window"). Το γράμμα X ήταν απλά το επόμενο γράμμα στο Λατινικό αλφάβητο.

Μπορείτε να αναφέρεσθε στο X με τα ονόματα "X", "X Window System", "X11", καθώς και με μερικούς άλλους όρους. Προσοχή όμως: κάποιοι άνθρωποι θεωρούν προσβλητικό τον όρο "X

Windows". Για περισσότερες πληροφορίες σχετικά με αυτό, δείτε τη σελίδα manual X(7).

7.2.2. Το Μοντέλο Πελάτη/Διακομιστή των X11

Το περιβάλλον X11 έχει σχεδιαστεί από την αρχή έτσι ώστε να έχει εγγενή δικτυακή υποστήριξη, με βάση ένα μοντέλο "πελάτη-διακομιστή".

Στο μοντέλο λειτουργίας του X11, ο "διακομιστής X" εκτελείται στον υπολογιστή στον οποίο έχει συνδεθεί το πληκτρολόγιο, η οθόνη και το ποντίκι. Ο διακομιστής X είναι υπεύθυνος για τη διαχείριση της οθόνης, της εισόδου από το πληκτρολόγιο, το ποντίκι, και άλλες συσκευές εισόδου ή εξόδου (για παράδειγμα, μια "ταμπλέτα" μπορεί να χρησιμοποιείται ως συσκευή εισόδου και ένας video-προβολέας ως εναλλακτική συσκευή εξόδου). Κάθε εφαρμογή X (π.χ. το XTerm ή το getenv(3)) είναι ένας "πελάτης". Ένας πελάτης στέλνει μηνύματα στον διακομιστή όπως "Παρακαλώ σχεδίασε ένα παράθυρο σε αυτές τις συντεταγμένες", και ο διακομιστής στέλνει πίσω μηνύματα όπως "Ο χρήστης μόλις πάτησε το πλήκτρο OK".

Σε ένα σπίτι ή ένα μικρό γραφείο, ο διακομιστής και οι πελάτες X συχνά εκτελούνται στον ίδιο υπολογιστή. Όμως, είναι απόλυτα εφικτό να εκτελείται ο διακομιστής X σε έναν λιγότερο ισχυρό επιτραπέζιο υπολογιστή, και να εκτελούνται οι εφαρμογές X (οι πελάτες) σε ένα, ας πούμε, ισχυρό και ακριβό μηχάνημα που εξυπηρετεί το γραφείο. Σε αυτό το σενάριο η επικοινωνία μεταξύ των πελατών X και του διακομιστή γίνεται μέσω δικτύου.

Αυτό προκαλεί σύγχυση σε ορισμένους, επειδή η ορολογία του X είναι ακριβώς αντίθετη από ότι περίμεναν. Οι χρήστες συνήθως περιμένουν ο "διακομιστής X" να είναι ένα μεγάλο ισχυρό μηχάνημα σε ένα δωμάτιο και ο "πελάτης X" να είναι το μηχάνημα του γραφείου τους.

Είναι σημαντικό να θυμάστε ότι ο διακομιστής X είναι το μηχάνημα με την οθόνη και το πληκτρολόγιο, και οι πελάτες X είναι τα προγράμματα που εμφανίζουν τα παράθυρα.

Δεν υπάρχει τίποτα στο πρωτόκολλο που να αναγκάζει τα μηχανήματα των πελατών και του διακομιστή να εκτελούνται στο ίδιο λειτουργικό σύστημα, ή ακόμη να εκτελούνται στον ίδιο τύπο υπολογιστή. Είναι απόλυτα εφικτό να εκτελείται ένας διακομιστής X στα Microsoft® Windows® ή στο Mac OS® της Apple, και υπάρχουν διαθέσιμες διάφορες ελεύθερες και εμπορικές εφαρμογές που κάνουν ακριβώς αυτό.

7.2.3. Ο Διαχειριστής Παραθύρων

Η φιλοσοφία σχεδιασμού του X μοιάζει πολύ με την φιλοσοφία σχεδιασμού του UNIX®, "εργαλεία, όχι πολιτική". Αυτό σημαίνει ότι το X δεν προσπαθεί να υπαγορεύσει πως θα υλοποιηθεί μια εργασία. Αντίθετα, παρέχονται εργαλεία στον χρήστη, και είναι δική του ευθύνη να αποφασίσει πως θα τα χρησιμοποιήσει.

Αυτή η φιλοσοφία επεκτείνεται στο ότι το X δεν υπαγορεύει πως πρέπει να εμφανίζονται τα παράθυρα στην οθόνη, πως θα μετακινηθούν με το ποντίκι, τι συνδυασμοί πλήκτρων πρέπει να χρησιμοποιηθούν για να μετακινηθούμε μεταξύ των παραθύρων (π.χ., `Alt` + `Tab`, στην περίπτωση των Microsoft® Windows®), πώς πρέπει να μοιάζουν οι μπάρες τίτλων σε κάθε παράθυρο, αν θα έχουν ή όχι πλήκτρα κλεισίματος πάνω τους, κ.ο.κ.

Αντίθετα, το X αναθέτει αυτήν την ευθύνη σε μία εφαρμογή που ονομάζεται "Διαχειριστής

Παραθύρων". Υπάρχουν πάρα πολλοί διαχειριστές παραθύρων διαθέσιμοι για το περιβάλλον X. Ορισμένοι από αυτούς είναι οι: AfterStep, Blackbox, ctwm, Enlightenment, fvwm, Sawfish, twm, Window Maker, και πολλοί άλλοι. Κάθε ένας από αυτούς τους διαχειριστές παραθύρων έχει διαφορετική αίσθηση και εμφάνιση. Μερικοί από αυτούς υποστηρίζουν "εικονικές επιφάνειες εργασίας", μερικοί επιτρέπουν προσαρμοσμένους συνδυασμούς πλήκτρων για την διαχείριση της επιφάνειας εργασίας, μερικοί έχουν ένα πλήκτρο "Start" ή κάτι παρόμοιο, μερικοί υποστηρίζουν "θέματα" (themes), επιτρέποντας την ολοκληρωτική αλλαγή εμφάνισης με την εφαρμογή ενός νέου θέματος. Οι διαχειριστές παραθύρων που έχουμε αναφέρει ως τώρα, και πολλοί άλλοι, είναι διαθέσιμοι στην κατηγορία x11-wm της Συλλογής των Ports.

Επιπλέον, τα δύο πιο δημοφιλή ολοκληρωμένα περιβάλλοντα εργασίας, το KDE και το GNOME, έχουν τον δικό τους διαχειριστή παραθύρων που είναι ενσωματωμένος με το υπόλοιπο περιβάλλον εργασίας.

Κάθε διαχειριστής παραθύρων έχει επίσης και διαφορετικό μηχανισμό ρύθμισης: μερικοί ρυθμίζονται συμπληρώνοντας με χειροκίνητο τρόπο ένα αρχείο ρυθμίσεων, άλλοι διαθέτουν γραφικά εργαλεία για τις περισσότερες ρυθμίσεις. Υπάρχει ακόμα κι ένας (Sawfish) που έχει αρχείο ρυθμίσεων γραμμένο σε μια διάλεκτο της γλώσσας Lisp.

Πολιτική Εστίασης

Άλλο ένα θέμα για το οποίο είναι υπεύθυνος ο διαχειριστής παραθύρων είναι η "πολιτική εστίασης" του ποντικιού. Κάθε σύστημα παραθύρων χρειάζεται κάποιο τρόπο επιλογής του παραθύρου που θα δέχεται αυτά που πληκτρολογούνται, και θα πρέπει να φαίνεται κάπως ότι αυτό το παράθυρο είναι ενεργό.

Μία γνωστή πολιτική εστίασης λέγεται "click-to-focus". Αυτό το μοντέλο χρησιμοποιείται στα Microsoft® Windows®, όπου ένα παράθυρο γίνεται ενεργό αν δεχτεί ένα πάτημα του ποντικιού.

Το X δεν υποστηρίζει καμία συγκεκριμένη πολιτική εστίασης. Αντίθετα, ο διαχειριστής παραθύρων ελέγχει ποίο παράθυρο έχει εστιαστεί κάθε στιγμή. Διαφορετικοί διαχειριστές παραθύρων υποστηρίζουν διαφορετικές μεθόδους εστίασης. Όλοι τους υποστηρίζουν την μέθοδο click to focus, και οι περισσότεροι από αυτούς υποστηρίζουν και αρκετές άλλες.

Οι πιο δημοφιλείς μέθοδοι εστίασης είναι:

focus-follows-mouse

Το παράθυρο που βρίσκεται κάτω από τον δείκτη του ποντικιού είναι το παράθυρο που έχει την εστίαση. Το ενεργό παράθυρο δεν είναι απαραίτητο να είναι αυτό που βρίσκεται πάνω από όλα τα άλλα. Η εστίαση αλλάζει με την στόχευση ενός άλλου παραθύρου, χωρίς να είναι απαραίτητο το κλικ πάνω του.

sloppy-focus

Αυτή η πολιτική είναι μια μικρή επέκταση του focus-follows-mouse. Με την πολιτική εστίασης focus-follows-mouse, αν το ποντίκι βρεθεί πάνω από το αρχικό (root) παράθυρο (ή το παρασκήνιο) δεν υπάρχει εστίαση σε κανένα παράθυρο, και ότι πληκτρολογείται απλώς χάνεται. Με τη sloppy-focus, η εστίαση αλλάζει μόνο αν ο δείκτης βρεθεί πάνω από ένα νέο παράθυρο, και όχι

όταν φεύγει από το τρέχον παράθυρο.

click-to-focus

Το ενεργό παράθυρο επιλέγεται με κλικ του ποντικιού. Το παράθυρο τότε "ανασηκώνεται", και εμφανίζεται μπροστά από όλα τα άλλα παράθυρα. Ότι πληκτρολογηθεί θα οδηγηθεί σε αυτό το παράθυρο, ακόμα και αν ο δείκτης μετακινηθεί σε άλλο παράθυρο.

Πολλοί διαχειριστές παραθύρων υποστηρίζουν ακόμα πιο εξωτικές πολιτικές εστίασης, καθώς και παραλλαγές των παραπάνω. Συμβουλευθείτε την τεκμηρίωση του εκάστοτε διαχειριστή παραθύρων για περισσότερες λεπτομέρειες.

7.2.4. Γραφικά Στοιχεία Διεπαφής (Widgets)

Η προσέγγιση του X να διαθέτει εργαλεία και όχι να υπαγορεύει τον τρόπο χρήσης τους, διευρύνεται και στα γραφικά στοιχεία διεπαφής (widgets) που φαίνονται στην οθόνη σε κάθε εφαρμογή.

Τα "widgets" είναι ένας όρος για όλα τα αντικείμενα στο περιβάλλον του χρήστη που μπορεί κάποιος να κάνει κλικ ή να τα χειριστεί με κάποιον τρόπο: πλήκτρα, πλαίσια επιλογής, πλήκτρα εναλλαγής, εικονίδια, λίστες, και άλλα. Τα Microsoft® Windows® τα ονομάζουν "controls (χειριστήρια)".

Τα Microsoft® Windows® και το Mac OS® της Apple έχουν και τα δύο πολύ αυστηρή πολιτική γραφικών στοιχείων διεπαφής. Οι προγραμματιστές εφαρμογών πρέπει υποτίθεται να εξασφαλίσουν ότι οι εφαρμογές τους θα έχουν κοινή αίσθηση και εμφάνιση (look and feel). Στο X, δεν θεωρήθηκε απαραίτητο να γίνει επιβολή ενός συγκεκριμένου στυλ γραφικών, ή να τεθούν κάποια υποχρεωτικά γραφικά στοιχεία διεπαφής.

Σαν αποτέλεσμα, μην περιμένετε τις εφαρμογές για X να έχουν κοινή εμφάνιση. Υπάρχουν διάφορες δημοφιλείς συλλογές γραφικών στοιχείων διεπαφής και παραλλαγές τους, συμπεριλαμβανομένης και της αυθεντικής Athena συλλογής γραφικών στοιχείων διεπαφής του MIT, Motif® (παραλλαγή της οποίας είναι και η συλλογή γραφικών στοιχείων διεπαφής των Microsoft® Windows®, με λοξές γωνίες και τρεις διαβαθμίσεις του γκρι), το OpenLook, και άλλα.

Οι περισσότερες νέες X εφαρμογές σήμερα χρησιμοποιούν μια συλλογή γραφικών στοιχείων διεπαφής με μοντέρνα εμφάνιση, είτε το Qt, που χρησιμοποιείται από το KDE, είτε το GTK+, που χρησιμοποιείται από το GNOME. Από αυτή την άποψη, υπάρχει κάποια σύγκλιση στην εμφάνιση του UNIX® desktop, το οποίο οπωσδήποτε κάνει τα πράγματα ευκολότερα για τον νέο χρήστη.

7.3. Εγκατάσταση του X11

Το Xorg είναι η προεπιλεγμένη υλοποίηση X11 για το FreeBSD. Το Xorg είναι ο διακομιστής X της υλοποίησης X Window System του X.Org Foundation, και είναι ανοικτού κώδικα. Ο Xorg είναι βασισμένος στον κώδικα του XFree86™ 4.4RC2 και του X11R6.6. Η έκδοση του Xorg που διατίθεται από την Συλλογή των Ports του FreeBSD είναι η 7.7.

Για να μεταγλωττίσετε και να εγκαταστήσετε το Xorg από την Συλλογή των Ports:

```
# cd /usr/ports/x11/xorg
# make install clean
```

Για να μεταγλωττίσετε ολόκληρο το Xorg σιγουρευθείτε ότι έχετε το λιγότερο 4 GB ελεύθερο χώρο διαθέσιμο.

Εναλλακτικά, το X11 μπορεί να εγκατασταθεί άμεσα από πακέτα. Υπάρχουν διαθέσιμα έτοιμα πακέτα του X11 για χρήση με το εργαλείο pkg_add(1). Αν χρησιμοποιήσετε τη δυνατότητα του pkg_add(1) για λήψη μέσω δικτύου, δεν θα πρέπει στην γραμμή εντολών να δώσετε τον αριθμό έκδοσης (version number) του πακέτου. Το pkg_add(1) θα "κατεβάσει" αυτόματα την τελευταία έκδοση της εφαρμογής.

Έτσι, για να γίνει η λήψη και η εγκατάσταση του Xorg, απλώς εκτελέστε:

```
# pkg_add -r xorg
```

Τα παραπάνω παραδείγματα θα εγκαταστήσουν ολόκληρη την διανομή X11 που περιλαμβάνει διακομιστές, πελάτες, γραμματοσειρές κλπ. Διατίθενται επίσης ξεχωριστά, τμηματικά πακέτα και ports για το X11.

Για να εγκαταστήσετε την ελάχιστη δυνατή διανομή X11, μπορείτε εναλλακτικά να χρησιμοποιήσετε το port x11/xorg-minimal.

Το υπόλοιπο του κεφαλαίου θα σας εξηγήσει πως ρυθμίζεται το X11, και πως να στήσετε ένα παραγωγικό desktop περιβάλλον.

7.4. Ρύθμιση του X11

7.4.1. Πριν ξεκινήσετε

Στις περισσότερες περιπτώσεις, το X11 ρυθμίζεται αυτόματα. Αν το σύστημα σας είναι παλιό ή διαθέτει εξεζητημένα εξαρτήματα, θα είναι χρήσιμο να μαζέψετε κάποιες επιπλέον πληροφορίες σχετικά με το υλικό σας πριν ξεκινήσετε τη ρύθμιση.

- Συχνότητες λειτουργίας της οθόνης σας
- Chipset της κάρτας γραφικών
- Μνήμη της κάρτας γραφικών

Η ανάλυση της οθόνης και ο ρυθμός ανανέωσης προσδιορίζονται από τις οριζόντιες και κατακόρυφες συχνότητες συγχρονισμού της οθόνης. Σχεδόν όλες οι οθόνες υποστηρίζουν αυτόματη ανίχνευση αυτών των τιμών. Κάποια μοντέλα δεν παρέχουν αυτές τις τιμές τις οποίες θα πρέπει να βρείτε στο εγχειρίδιο της οθόνης ή στην ιστοσελίδα του κατασκευαστή.

Το chipset (ολοκληρωμένο κύκλωμα) της κάρτας γραφικών ανιχνεύεται επίσης αυτόματα και χρησιμοποιείται για να επιλεγεί το κατάλληλο πρόγραμμα οδήγησης. Είναι ωστόσο χρήσιμο να

γνωρίζετε το μοντέλο για την περίπτωση που η αυτόματη ανίχνευση δεν είναι επιτυχής.

Η μνήμη της κάρτας γραφικών καθορίζει την ανάλυση και το βάθος χρώματος στο οποίο μπορεί να δουλέψει το σύστημα.

7.4.2. Ρύθμιση του X11

Το Xorg χρησιμοποιεί το HAL για την αυτόματη ανίχνευση του πληκτρολογίου και του ποντικιού. Τα ports sysutils/hal και devel/dbus εγκαθίστανται ως εξαρτήσεις του x11/xorg, αλλά θα πρέπει να ενεργοποιηθούν με τις ακόλουθες εγγραφές στο /etc/rc.conf:

```
hald_enable="YES"
dbus_enable="YES"
```

Θα πρέπει να ξεκινήσετε τις υπηρεσίες αυτές (είτε χειροκίνητα, είτε κάνοντας επανεκκίνηση) πριν συνεχίσετε με τη ρύθμιση ή την χρήση του Xorg.

Το Xorg μπορεί συχνά να λειτουργήσει χωρίς καμιά επιπλέον ρύθμιση, γράφοντας απλώς στη γραμμή εντολών:

```
% startx
```

Σε κάποιες περιπτώσεις, η αυτόματη ρύθμιση μπορεί να μη λειτουργήσει σωστά, ή να μη ρυθμίσει τις συσκευές ακριβώς όπως επιθυμείτε. Στις περιπτώσεις αυτές, θα χρειαστεί να κάνετε χειροκίνητες ρυθμίσεις.

Κάποια γραφικά περιβάλλοντα, όπως το GNOME το KDE ή το XFCE, διαθέτουν εργαλεία που επιτρέπουν στο χρήστη να ρυθμίσει με εύκολο τρόπο διάφορες παραμέτρους της οθόνης, όπως η ανάλυση. Αν η προεπιλεγμένη ρύθμιση δεν είναι αποδεκτή, και σκοπεύετε να εγκαταστήσετε κάποιο από αυτά τα περιβάλλοντα, μπορείτε να συνεχίσετε με την εγκατάσταση του, και να ολοκληρώσετε τις ρυθμίσεις σας χρησιμοποιώντας το κατάλληλο γραφικό εργαλείο.

Το πρώτο βήμα είναι η δημιουργία ενός αρχικού αρχείου ρυθμίσεων. Ως root, απλώς εκτελέστε:

```
# Xorg -configure
```

Αυτό θα δημιουργήσει ένα πρότυπο αρχείο ρυθμίσεων του X11 στον κατάλογο /root με το όνομα xorg.conf.new (είτε χρησιμοποιήσετε το su(1) είτε συνδεθείτε απευθείας, η μεταβλητή καταλόγου $HOME αλλάζει δείχνοντας τον κατάλογο του root). Το X11 θα προσπαθήσει να ανιχνεύσει το υποσύστημα γραφικών του συστήματος και να δημιουργήσει ένα αρχείο ρυθμίσεων που θα φορτώνει τους σωστούς οδηγούς συσκευών για το υλικό που ανιχνεύθηκε στο σύστημα σας.

Το επόμενο βήμα είναι ο έλεγχος των υπάρχοντων ρυθμίσεων για να επιβεβαιώσετε ότι το Xorg λειτουργεί με το υποσύστημα γραφικών του συστήματος σας. Πληκτρολογήστε:

```
# Xorg -config xorg.conf.new -retro
```

Εάν εμφανιστεί ένα μαύρο και γκρι πλέγμα και ένας δείκτης ποντικιού με μορφή X, η ρύθμιση ήταν επιτυχής. Για να τερματίσετε τη δοκιμή, μεταβείτε στην εικονική κονσόλα από την οποία την ξεκινήσατε, πιέζοντας `Ctrl` + `Alt` + `Fn` (`F1` για την πρώτη εικονική κονσόλα) και πιέστε `Ctrl` + `C`.

Μπορείτε επίσης να χρησιμοποιήσετε τον συνδυασμό πλήκτρων `Ctrl` + `Alt` + `Backspace` για τον τερματισμό του προγράμματος. Για να τον ενεργοποιήσετε, δώστε την παρακάτω εντολή σε κάποιο τερματικό του X:

```
% setxkbmap -option terminate:ctrl_alt_bksp
```

Εναλλακτικά, δημιουργήστε ένα αρχείο ρυθμίσεων πληκτρολογίου για το hald με την ονομασία x11-input.fdi και αποθηκεύστε το στον κατάλογο /usr/local/etc/hal/fdi/policy. Το αρχείο αυτό θα πρέπει να περιέχει τις παρακάτω γραμμές:

```
<?xml version="1.0" encoding="utf-8"?>
<deviceinfo version="0.2">
  <device>
    <match key="info.capabilities" contains="input.keyboard">
      <merge key="input.x11_options.XkbOptions"
type="string">terminate:ctrl_alt_bksp</merge>
    </match>
  </device>
</deviceinfo>
```

Θα χρειαστεί να επανεκκινήσετε το μηχάνημα σας για να εξαναγκάσετε το hald να διαβάσει αυτό το αρχείο.

Θα πρέπει επίσης να προσθέσετε την παρακάτω γραμμή στο αρχείο xorg.conf.new, στην ενότητα `ServerLayout` ή `ServerFlags`:

```
Option  "DontZap"   "off"
```

Αν το ποντίκι δεν λειτουργεί, θα χρειαστεί να το ρυθμίσετε πριν συνεχίσετε. Δείτε το Ρυθμίσεις Ποντικιού (Mouse Settings) στο κεφάλαιο εγκατάστασης του FreeBSD. Επιπρόσθετα, στις πρόσφατες εκδόσεις του Xorg, οι ενότητες `InputDevice` στο xorg.conf αγνοούνται καθώς γίνεται χρήση των συσκευών που ανιχνεύθηκαν αυτόματα. Για να επαναφέρετε την παλιά συμπεριφορά, προσθέστε την παρακάτω γραμμή στην ενότητα `ServerLayout` ή `ServerFlags` του αρχείου ρυθμίσεων:

```
Option "AutoAddDevices" "false"
```

Θα μπορείτε έπειτα να ρυθμίσετε τις συσκευές εισόδου όπως στις προηγούμενες εκδόσεις του Xorg,

χρησιμοποιώντας και όποιες άλλες επιλογές χρειάζεστε (π.χ. εναλλαγή πληκτρολογίου).

Όπως εξηγήσαμε και προηγουμένως, ο δαίμονας hald αναλαμβάνει να ανιχνεύσει αυτόματα το πληκτρολόγιο σας. Υπάρχει περίπτωση να μην γίνει σωστή ανίχνευση του μοντέλου ή της διάταξης, ωστόσο κάποια γραφικά περιβάλλοντα όπως το GNOME το KDE και το Xfce παρέχουν τα δικά τους εργαλεία για τη ρύθμιση του. Μπορείτε όμως να ρυθμίσετε τις ιδιότητες του πληκτρολογίου και απευθείας, είτε μέσω του βοηθητικού προγράμματος setxkbmap(1) είτε με την προσθήκη ενός κανόνα στο hald.

Για παράδειγμα, αν κάποιος θέλει να χρησιμοποιήσει ένα πληκτρολόγιο 102 πλήκτρων με γαλλική διάταξη, θα πρέπει να δημιουργήσει ένα αρχείο ρυθμίσεων για το hald με το όνομα x11-input.fdi και να το αποθηκεύσει στον κατάλογο /usr/local/etc/hal/fdi/policy. Το αρχείο αυτό θα περιέχει τις παρακάτω γραμμές:

```
<?xml version="1.0" encoding="utf-8"?>
<deviceinfo version="0.2">
  <device>
    <match key="info.capabilities" contains="input.keyboard">
      <merge key="input.x11_options.XkbModel"
type="string">pc102</merge>
      <merge key="input.x11_options.XkbLayout" type="string">fr</merge>
    </match>
  </device>
</deviceinfo>
```

Αν το αρχείο αυτό υπάρχει ήδη, απλώς αντιγράψτε τις παραπάνω γραμμές μέσα στο υπάρχον περιεχόμενο.

Θα πρέπει να επανεκκινήσετε το μηχάνημα σας για να εξαναγκάσετε το hald να διαβάσει το αρχείο.

Μπορείτε επίσης να κάνετε την ίδια ρύθμιση μέσα από ένα τερματικό στα X ή ακόμα και από ένα script, εκτελώντας την παρακάτω εντολή:

```
% setxkbmap -model pc102 -layout fr
```

Μπορείτε να βρείτε τις διαθέσιμες επιλογές πληκτρολογίων και διατάξεων στο αρχείο /usr/local/shared/X11/xkb/rules/base.lst.

Έπειτα, προσαρμόστε το αρχείο ρυθμίσεων xorg.conf.new στις προτιμήσεις σας. Ανοίξτε το με έναν συντάκτη κειμένου όπως ο emacs(1) ή ο ee(1). Αν η οθόνη σας είναι παλιό ή εξεζητημένο μοντέλο και δεν υποστηρίζει αυτόματη ανίχνευση των συχνοτήτων λειτουργίας της, μπορείτε να τις καταχωρίσετε χειροκίνητα στο xorg.conf.new στην ενότητα "Monitor":

```
Section "Monitor"
        Identifier   "Monitor0"
```

```
        VendorName   "Monitor Vendor"
        ModelName    "Monitor Model"
        HorizSync    30-107
        VertRefresh  48-120
EndSection
```

Οι περισσότερες οθόνες υποστηρίζουν αυτόματη ανίχνευση των συχνοτήτων λειτουργίας, καθιστώντας έτσι αχρείαστη τη χειροκίνητη καταχώριση αυτών των τιμών. Για τις λίγες περιπτώσεις που δε υποστηρίζεται η αυτόματη ανίχνευση, συνίσταται να χρησιμοποιήσετε τις τιμές που δίνει ο κατασκευαστής για να αποφύγετε πιθανές βλάβες στο υλικό σας.

Το X επιτρέπει τη χρήση των δυνατοτήτων DPMS (Energy Star) σε οθόνες που υποστηρίζουν την αντίστοιχη λειτουργία. Το πρόγραμμα xset(1) ελέγχει τους χρόνους και μπορεί να επιβάλλει τις καταστάσεις standby, suspend, ή off. Αν θέλετε να ενεργοποιήσετε τις δυνατότητες DPMS της οθόνης σας, πρέπει να προσθέσετε την ακόλουθη γραμμή στο Section monitor:

```
        Option       "DPMS"
```

Όσο το αρχείο ρυθμίσεων xorg.conf.new είναι ακόμα ανοικτό σε έναν συντάκτη κειμένου, επιλέξτε την ανάλυση και το βάθος χρωμάτων που επιθυμείτε. Αυτό καθορίζεται στο Section "Screen":

```
Section "Screen"
        Identifier "Screen0"
        Device     "Card0"
        Monitor    "Monitor0"
        DefaultDepth 24
        SubSection "Display"
                Viewport  0 0
                Depth     24
                Modes     "1024x768"
        EndSubSection
EndSection
```

Η μεταβλητή DefaultDepth ορίζει το προεπιλεγμένο βάθος χρώματος που θα χρησιμοποιηθεί. Μπορείτε να την παρακάμψετε με τον διακόπτη -depth στη γραμμή εντολών του Xorg(1). Η επιλογή Modes ορίζει την ανάλυση με την οποία θα λειτουργεί η οθόνη σε ένα συγκεκριμένο βάθος χρωμάτων. Προσέξτε ότι υποστηρίζονται μόνο κανονικές καταστάσεις VESA, όπως ορίζονται από το υποσύστημα γραφικών του συστήματος. Στο παραπάνω παράδειγμα, το καθορισμένο βάθος χρωμάτων είναι εικοσιτέσσερα bits ανά pixel. Σε αυτό το βάθος χρωμάτων, η αποδεκτή ανάλυση είναι 1024X768 pixels.

Τέλος, αποθηκεύστε το αρχείο ρυθμίσεων και ελέγξτε το με την μέθοδο ελέγχου που εξηγήσαμε παραπάνω.

Ένα από τα εργαλεία που μπορεί να σας βοηθήσουν κατά την διαδικασία επίλυσης προβλημάτων, είναι τα αρχεία X11 log, που περιέχουν πληροφορίες για κάθε συσκευή που επικοινωνεί με τον διακομιστή X11. Τα αρχεία Xorg log ονομάζονται

με την μορφή /var/log/Xorg.0.log. Το ακριβές όνομα ενός log μπορεί να είναι Xorg.0.log έως Xorg.8.log και πάει λέγοντας.

Αν όλα είναι καλά, το αρχείο ρυθμίσεων πρέπει να τοποθετηθεί σε μια κοινή τοποθεσία ώστε να εντοπίζεται από το Xorg(1). Αυτή συνήθως είναι η /etc/X11/xorg.conf ή /usr/local/etc/X11/xorg.conf.

```
# cp xorg.conf.new /etc/X11/xorg.conf
```

Η διαδικασία ρύθμισης του X11 έχει τώρα ολοκληρωθεί. Το Xorg μπορείτε να το ξεκινήσετε με το βοηθητικό πρόγραμμα startx(1). Ο διακομιστής X11 μπορεί επίσης να εκκινήσει με τη βοήθεια του xdm(1).

7.4.3. Εξειδικευμένα Θέματα Ρυθμίσεων

7.4.3.1. Ρυθμίσεις για τα Intel® `i810` Graphics Chipsets

Για να χρησιμοποιήσετε κάρτα βασισμένη στα Intel® i810 integrated chipsets, απαιτείται το agpgart, η διεπαφή προγραμματισμού των X11 για το AGP. Δείτε την σελίδα manual του προγράμματος οδήγησης agp(4) για περισσότερες πληροφορίες.

Με αυτό τον τρόπο, η ρύθμιση του υλικού σας θα μπορεί να γίνει όπως και σε κάθε άλλη κάρτα γραφικών. Προσοχή, σε συστήματα χωρίς ενσωματωμένο τον οδηγό agp(4), ο οδηγός δεν θα φορτωθεί με την εντολή kldload(8). Ο οδηγός αυτός πρέπει να βρίσκεται στον πυρήνα κατά την εκκίνηση, είτε στατικά μεταγλωττισμένος, είτε με χρήση του /boot/loader.conf.

7.4.3.2. Προσθέτοντας μια Widescreen Επίπεδη Οθόνη

Αυτό το τμήμα προϋποθέτει μερικές γνώσεις εξειδικευμένων ρυθμίσεων. Αν οι προσπάθειες με τα συνήθη εργαλεία ρυθμίσεων δεν καταλήξουν σε μια ρύθμιση που να λειτουργεί, υπάρχουν αρκετές πληροφορίες στα αρχεία log που μπορούν να σας βοηθήσουν. Ωστόσο, είναι απαραίτητη η χρήση ενός συντάκτη κειμένου.

Οι τρέχουσες αναλύσεις widescreen (WSXGA, WSXGA+, WUXGA, WXGA, WXGA+, κ.α.) υποστηρίζουν formats και aspect ratios (αναλογίες) 16:10 και 16:9 που μπορεί να δημιουργήσουν προβλήματα. Παραδείγματα μερικών κοινών αναλύσεων για αναλογία 16:10 είναι τα:

- 2560x1600
- 1920x1200
- 1680x1050
- 1440x900
- 1280x800

Κάποια στιγμή, η ρύθμιση θα γίνεται πολύ απλά προσθέτοντας την ανάλυση ως ένα πιθανό `Mode` στο `Section "Screen"` όπως εδώ:

```
Section "Screen"
```

```
Identifier "Screen0"
Device     "Card0"
Monitor    "Monitor0"
DefaultDepth 24
SubSection "Display"
    Viewport  0 0
    Depth     24
    Modes     "1680x1050"
EndSubSection
EndSection
```

Το Xorg είναι αρκετά έξυπνο ώστε να ανακτήσει τις πληροφορίες της ανάλυσης της widescreen οθόνης μέσω των πληροφοριών I2C/DDC, γνωρίζοντας έτσι τι μπορεί να χειριστεί η οθόνη όσο αφορά τις συχνότητες και τις αναλύσεις.

Αν αυτές οι `ModeLines` δεν υπάρχουν στους οδηγούς, μπορεί να χρειαστεί να τις δώσετε εσείς στο Xorg. Χρησιμοποιώντας το /var/log/Xorg.0.log μπορείτε να ανακτήσετε αρκετές πληροφορίες ώστε να δημιουργήσετε μόνοι σας ένα `ModeLine` που να λειτουργεί. Απλώς αναζητήστε πληροφορίες που θα μοιάζουν με αυτό:

```
(II) MGA(0): Supported additional Video Mode:
(II) MGA(0): clock: 146.2 MHz   Image Size:  433 x 271 mm
(II) MGA(0): h_active: 1680  h_sync: 1784  h_sync_end 1960 h_blank_end 2240 h_border:
0
(II) MGA(0): v_active: 1050  v_sync: 1053  v_sync_end 1059 v_blanking: 1089 v_border:
0
(II) MGA(0): Ranges: V min: 48  V max: 85 Hz, H min: 30  H max: 94 kHz, PixClock max
170 MHz
```

Αυτές ονομάζονται πληροφορίες EDID. Η δημιουργία ενός `ModeLine` από αυτές, γίνεται βάζοντας απλώς τους αριθμούς στη σωστή σειρά:

```
ModeLine <name> <clock> <4 horiz. timings> <4 vert. timings>
```

Τελικά, το `ModeLine` στο `Section "Monitor"` στο παράδειγμα μας θα μοιάζει με αυτό:

```
Section "Monitor"
Identifier      "Monitor1"
VendorName      "Bigname"
ModelName       "BestModel"
ModeLine        "1680x1050" 146.2 1680 1784 1960 2240 1050 1053 1059 1089
Option          "DPMS"
EndSection
```

Τώρα που έχετε τελειώσει με αυτά τα απλά βήματα, το X θα πρέπει να λειτουργήσει στη νέα widescreen οθόνη σας.

7.5. Χρήση Γραμματοσειρών στο X11

7.5.1. Γραμματοσειρές τύπου Type1

Οι προκαθορισμένες γραμματοσειρές που συνοδεύουν το X11 δεν είναι ιδανικές για εφαρμογές επιτραπέζιας τυπογραφίας. Οι μεγάλες γραμματοσειρές παρουσίασης φαίνονται οδοντωτές και ερασιτεχνικές, και οι μικρές γραμματοσειρές στο getenv(3) είναι σχεδόν ακατάληπτες. Ευτυχώς όμως, υπάρχουν διαθέσιμες αρκετές, υψηλής ποιότητας γραμματοσειρές Type1 (PostScript®) που μπορούν να χρησιμοποιηθούν άμεσα από το X11. Για παράδειγμα, η συλλογή γραμματοσειρών URW (x11-fonts/urwfonts) περιέχει εκδόσεις υψηλής ποιότητας των συνηθισμένων type1 γραμματοσειρών (Times Roman™, Helvetica™, Palatino™ και άλλες). Η συλλογή Freefonts (x11-fonts/freefonts) περιέχει πολλές περισσότερες γραμματοσειρές, αλλά οι περισσότερες από αυτές είναι για λογισμικό γραφικών όπως το Gimp, και δεν είναι κατάλληλες για γραμματοσειρές οθόνης. Ακόμη, το X11 μπορεί με ελάχιστο κόπο να ρυθμιστεί ώστε να χρησιμοποιεί TrueType® γραμματοσειρές. Για περισσότερες λεπτομέρειες, δείτε την σελίδα manual X(7) ή το τμήμα σχετικά με τις γραμματοσειρές TrueType®.

Για να εγκαταστήσετε τις παραπάνω συλλογές γραμματοσειρών Type1 από την Συλλογή των Ports, εκτελέστε τις παρακάτω εντολές:

```
# cd /usr/ports/x11-fonts/urwfonts
# make install clean
```

Με παρόμοιο τρόπο μπορείτε να εγκαταστήσετε και την freefont ή άλλες συλλογές. Για να ανιχνεύσει ο X server αυτές τις γραμματοσειρές, προσθέστε την κατάλληλη γραμμή στο αρχείο ρυθμίσεων του (/etc/X11/xorg.conf):

```
FontPath "/usr/local/lib/X11/fonts/URW/"
```

Εναλλακτικά, εκτελέστε στην γραμμή εντολών μιας συνόδου X:

```
% xset fp+ /usr/local/lib/X11/fonts/URW
% xset fp rehash
```

Αυτό θα λειτουργήσει, αλλά όταν τερματίσει η σύνοδος X, οι ρυθμίσεις θα χαθούν, εκτός αν προστεθούν στο αρχείο εκκίνησης (το ~/.xinitrc για μία συνηθισμένη σύνοδο μέσω `startx`, η το ~/.xsession αν συνδέεστε μέσω ενός γραφικού διαχειριστή σύνδεσης όπως ο XDM). Ένας ακόμη τρόπος είναι να χρησιμοποιήσετε το αρχείο /usr/local/etc/fonts/local.conf: δείτε το τμήμα anti-aliasing (εξομάλυνσης).

7.5.2. Γραμματοσειρές TrueType®

Το Xorg έχει ενσωματωμένη υποστήριξη απεικόνισης γραμματοσειρών TrueType®. Υπάρχουν δύο διαφορετικά modules (αρθρώματα) που μπορούν να ενεργοποιήσουν αυτήν την λειτουργία. Σε αυτό το παράδειγμα χρησιμοποιείται το freetype module επειδή είναι πιο συνεργάσιμο με τα άλλα back-

ends απεικόνισης γραμματοσειρών. Για να ενεργοποιήσετε το freetype module, απλώς προσθέστε την παρακάτω γραμμή στο τμήμα `"Module"` του αρχείου /etc/X11/xorg.conf.

```
Load  "freetype"
```

Τώρα, δημιουργήστε έναν κατάλογο για τις γραμματοσειρές TrueType® (για παράδειγμα, /usr/local/lib/X11/fonts/TrueType) και αντιγράψτε όλες τις γραμματοσειρές TrueType® σε αυτόν. Προσέξτε ότι οι γραμματοσειρές TrueType® δεν μπορούν να είναι από ένα σύστημα Macintosh® πρέπει να είναι σε μορφή UNIX®/MS-DOS®/Windows® για να λειτουργούν στο X11. Μόλις αντιγραφούν τα αρχεία στον κατάλογο, χρησιμοποιήστε το ttmkfdir για να δημιουργήσετε το αρχείο fonts.dir, ώστε ο X font renderer να γνωρίζει την ύπαρξη των νέων αυτών αρχείων. Το `ttmkfdir` διατίθεται από την Συλλογή των Ports του FreeBSD ως x11-fonts/ttmkfdir.

```
# cd /usr/local/lib/X11/fonts/TrueType
# ttmkfdir -o fonts.dir
```

Τώρα, προσθέστε τον κατάλογο TrueType® στη διαδρομή των fonts. Αυτό γίνεται με τον ίδιο τρόπο που περιγράψαμε παραπάνω στις Type1 γραμματοσειρές, χρησιμοποιώντας το

```
% xset fp+ /usr/local/lib/X11/fonts/TrueType
% xset fp rehash
```

ή απλά προσθέστε μια γραμμή `FontPath` στο αρχείο xorg.conf.

Αυτό ήταν. Τώρα ο getenv(3), το Gimp, το StarOffice™, και όλες οι άλλες εφαρμογές X πρέπει να αναγνωρίζουν τις εγκαταστημένες TrueType® γραμματοσειρές. Πολύ μικρές γραμματοσειρές (όπως αυτές που φαίνονται στο κείμενο μιας ιστοσελίδας σε υψηλή ανάλυση) και πολύ μεγάλες γραμματοσειρές (στο StarOffice™) θα φαίνονται τώρα πολύ καλύτερα.

7.5.3. Anti-Aliased Γραμματοσειρές

Όλες οι γραμματοσειρές X11 που βρίσκονται στο /usr/local/lib/X11/fonts/ και το ~/.fonts/ είναι αυτόματα διαθέσιμες για anti-aliasing σε εφαρμογές Xft-aware, συμπεριλαμβανομένων του KDE, GNOME και Firefox.

Για να ελέγξετε ποίες γραμματοσειρές είναι anti-aliased, ή να ρυθμίσετε τις ιδιότητες του anti-aliasing, δημιουργήστε (ή τροποποιήστε, αν ήδη υπάρχει) το αρχείο /usr/local/etc/fonts/local.conf. Μέσω αυτού του αρχείου μπορούν να ρυθμιστούν αρκετά εξειδικευμένα χαρακτηριστικά του συστήματος γραμματοσειρών Xft. Αυτό το τμήμα περιγράφει μόνο μερικές απλές δυνατότητες. Για περισσότερες λεπτομέρειες, δείτε το fonts-conf(5).

Το αρχείο αυτό πρέπει να είναι μορφής XML. Δώστε μεγάλη προσοχή στα πεζά / κεφαλαία, και σιγουρευθείτε ότι όλα τα tags έχουν κλείσει σωστά. Το αρχείο ξεκινά με την συνηθισμένη επικεφαλίδα XML και ένα ορισμό DOCTYPE, και έπειτα ακολουθεί το `<fontconfig>` tag:

```
      <?xml version="1.0"?>
```

```
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

Όπως είπαμε προηγουμένως, όλες οι γραμματοσειρές στο /usr/local/lib/X11/fonts/ όπως και στο ~/.fonts/ διατίθενται ήδη σε Xft-aware εφαρμογές. Αν θέλετε να προσθέσετε και άλλους καταλόγους εκτός από αυτούς τους δύο, προσθέστε μια γραμμή παρόμοια με αυτή που ακολουθεί στο /usr/local/etc/fonts/local.conf:

```
<dir>/path/to/my/fonts</dir>
```

Αφού προσθέσετε νέες γραμματοσειρές, και ειδικότερα νέους καταλόγους γραμματοσειρών, πρέπει να εκτελέσετε την ακόλουθη εντολή για να αναδημιουργήσετε την cache γραμματοσειρών:

```
# fc-cache -f
```

Το anti-aliasing κάνει τα άκρα ελαφρώς συγκεχυμένα, κάνοντας έτσι τα πολύ μικρά γράμματα πιο αναγνώσιμα, και αφαιρεί τις "κλίμακες" (σκαλοπάτια) από τα μεγάλα γράμματα, αλλά μπορεί να προκαλέσει ενοχλήσεις στα μάτια αν χρησιμοποιηθεί σε κανονικά μεγέθη. Για να εξαιρέσετε από το anti-aliasing μεγέθη γραμματοσειρών μικρότερα από 14 point, προσθέστε αυτές τις γραμμές:

```
        <match target="font">
            <test name="size" compare="less">
                <double>14</double>
            </test>
            <edit name="antialias" mode="assign">
                <bool>false</bool>
            </edit>
        </match>
        <match target="font">
            <test name="pixelsize" compare="less" qual="any">
                <double>14</double>
            </test>
            <edit mode="assign" name="antialias">
                <bool>false</bool>
            </edit>
        </match>
```

Το spacing (διαστήματα) σε μερικές monospaced γραμματοσειρές μπορεί επίσης να είναι ακατάλληλο όταν χρησιμοποιείται anti-aliasing. Αυτό φαίνεται να αποτελεί ιδιαίτερο πρόβλημα με το KDE. Μια διόρθωση για αυτό, είναι να επιβάλλετε στο spacing την τιμή 100 για αυτές τις γραμματοσειρές. Προσθέστε τις ακόλουθες γραμμές:

```
       <match target="pattern" name="family">
           <test qual="any" name="family">
               <string>fixed</string>
           </test>
```

```
            <edit name="family" mode="assign">
                <string>mono</string>
            </edit>
        </match>
        <match target="pattern" name="family">
            <test qual="any" name="family">
                <string>console</string>
            </test>
            <edit name="family" mode="assign">
                <string>mono</string>
            </edit>
        </match>
```

(αυτό μετονομάζει τα άλλα κοινά ονόματα των fixed γραμματοσειρών ως `"mono"`), και έπειτα προσθέστε:

```
        <match target="pattern" name="family">
            <test qual="any" name="family">
                <string>mono</string>
            </test>
            <edit name="spacing" mode="assign">
                <int>100</int>
            </edit>
        </match>
```

Συγκεκριμένες γραμματοσειρές, όπως οι Helvetica, μπορεί να εμφανίζουν πρόβλημα όταν είναι anti-aliased. Το πρόβλημα συχνά εκδηλώνεται ως μία γραμματοσειρά κομμένη κάθετα στην μέση. Στην χειρότερη περίπτωση, μπορεί να κάνει κάποιες εφαρμογές να καταρρεύσουν. Για να το αποφύγετε αυτό, μπορείτε να προσθέσετε το ακόλουθο στο local.conf:

```
        <match target="pattern" name="family">
            <test qual="any" name="family">
                <string>Helvetica</string>
            </test>
            <edit name="family" mode="assign">
                <string>sans-serif</string>
            </edit>
        </match>
```

Μόλις τελειώσετε την μετατροπή του local.conf σιγουρευθείτε ότι κλείσατε το αρχείο με το `</fontconfig>` tag. Αν δεν το κάνετε, οι αλλαγές σας θα αγνοηθούν.

Τέλος, οι χρήστες μπορούν να προσθέσουν τις δικές τους ρυθμίσεις μέσω των προσωπικών τους αρχείων .fonts.conf. Για να γίνει αυτό, κάθε χρήστης πρέπει απλώς να δημιουργήσει ένα ~/.fonts.conf. Αυτό το αρχείο πρέπει να είναι επίσης XML μορφής.

Κάτι τελευταίο: σε μία LCD οθόνη, μπορεί να είναι επιθυμητός ο δειγματισμός sub-pixel. Ο δειγματισμός χειρίζεται χωριστά τα (οριζόντια διαχωρισμένα) κόκκινα, πράσινα και μπλε στοιχεία

ώστε να βελτιώσει την οριζόντια ανάλυση. Τα αποτελέσματα μπορεί να είναι δραματικά καλύτερα. Για να τον ενεργοποιήσετε, προσθέστε την παρακάτω γραμμή κάπου στο αρχείο local.conf:

```
        <match target="font">
            <test qual="all" name="rgba">
                <const>unknown</const>
            </test>
            <edit name="rgba" mode="assign">
                <const>rgb</const>
            </edit>
        </match>
```

Ανάλογα με τον τύπο της οθόνης, το `rgb` μπορεί να χρειαστεί να αλλάξει σε `bgr`, `vrgb` ή `vbgr`: πειραματιστείτε και δείτε ποίο λειτουργεί καλύτερα.

7.6. Ο X Display Manager

7.6.1. Εισαγωγή

Ο X Display Manager (XDM) είναι ένα προαιρετικό μέρος του συστήματος X Windows που χρησιμοποιείται για διαχείριση συνδέσεων (logins). Αυτό είναι χρήσιμο σε πολλές περιπτώσεις, όπως σε απλά "X Terminals", σε desktop μηχανήματα, καθώς και σε διακομιστές μεγάλων δικτύων. Αφού το σύστημα X Windows είναι ανεξάρτητο πρωτοκόλλων και δικτύων, υπάρχει μεγάλο εύρος πιθανών ρυθμίσεων για την λειτουργία X πελατών και διακομιστών σε διαφορετικά μηχανήματα συνδεδεμένα σε ένα δίκτυο. Ο XDM παρέχει ένα γραφικό περιβάλλον για την επιλογή του διακομιστή με τον οποίο θα γίνει η σύνδεση, και για την είσοδο πληροφοριών πιστοποίησης όπως του ονόματος χρήστη και του κωδικού πρόσβασης.

Σκεφθείτε τον XDM ως μια εφαρμογή που παρέχει τις ίδιες δυνατότητες στον χρήστη με το εργαλείο getty(8) (δείτε το Ρύθμιση για λεπτομέρειες). Το XDM εκτελεί συνδέσεις (logins) στον διακομιστή και έπειτα εκτελεί ένα διαχειριστή συνεδρίας (session manager, συνήθως έναν X διαχειριστή παραθύρων, window manager) για λογαριασμό του χρήστη. Ο XDM έπειτα περιμένει να τερματίσει αυτό το πρόγραμμα, που σηματοδοτεί ότι ο χρήστης τελείωσε και πρέπει να αποσυνδεθεί. Σε αυτό το σημείο, ο XDM μπορεί να εμφανίσει ξανά την οθόνη εισόδου (login) και την οθόνη επιλογής γραφικής σύνδεσης ώστε να συνδεθεί ένας άλλος χρήστης.

7.6.2. Χρήση του XDM

Για να ξεκινήσετε να χρησιμοποιείτε το XDM, εγκαταστήστε το port x11/xdm (δεν εγκαθίσταται από προεπιλογή στις πρόσφατες εκδόσεις του Xorg). Μπορείτε έπειτα να βρείτε τον δαίμονα XDM στο /usr/local/bin/xdm. Αυτό το πρόγραμμα μπορεί να εκτελεστεί οποιαδήποτε στιγμή ως `root` και θα ξεκινήσει να διαχειρίζεται την οθόνη του X στο τοπικό μηχάνημα. Αν ο XDM πρέπει να εκτελείται κάθε φορά που εκκινείται το μηχάνημα, ένας βολικός τρόπος είναι η προσθήκη μιας γραμμής στο /etc/ttys. Για περισσότερες πληροφορίες σχετικά με την μορφή και την χρήση αυτού του αρχείου, δείτε το Προσθέτοντας μια Καταχώριση στο /etc/ttys. Υπάρχει μία γραμμή στο αρχικό /etc/ttys αρχείο για την εκτέλεση του XDM σε ένα εικονικό τερματικό:

```
ttyv8   "/usr/local/bin/xdm -nodaemon"  xterm   off secure
```

Αρχικά αυτή η λειτουργία είναι απενεργοποιημένη - για να την ενεργοποιήσετε αλλάξτε το πεδίο 5 από `off` σε `on` και επαννεκίνηστε το init(8) χρησιμοποιώντας τις οδηγίες του Εξαναγκάστε την init να Ξαναδιαβάσει το /etc/ttys. Το πρώτο πεδίο, το όνομα του τερματικού που θα διαχειρίζεται το πρόγραμμα, είναι το `ttyv8`. Αυτό σημαίνει ότι ο XDM θα εκτελείται στο 9ο εικονικό τερματικό.

7.6.3. Ρύθμιση του XDM

Ο κατάλογος ρυθμίσεων του XDM βρίσκεται στο /usr/local/lib/X11/xdm. Σε αυτόν τον κατάλογο υπάρχουν πολλά αρχεία που χρησιμοποιούνται για να αλλάξουν την συμπεριφορά και εμφάνιση του XDM. Τυπικά, θα βρείτε τα παρακάτω αρχεία:

Αρχείο	Περιγραφή
Xaccess	Κανόνες πιστοποίησης πελατών.
Xresources	Προκαθορισμένες τιμές X resource.
Xservers	Λίστα απομακρυσμένων και τοπικών οθονών (X displays) στις οποίες θα γίνεται διαχείριση.
Xsession	Προεπιλεγμένο script συνόδων για logins.
Xsetup_*	Script για την εκτέλεση εντολών πριν την εμφάνιση του περιβάλλοντος σύνδεσης (login screen).
xdm-config	Ρυθμίσεις για όλες τις απεικονίσεις (displays) που εκτελούνται σε αυτό το μηχάνημα.
xdm-errors	Λάθη που δημιουργούνται από το πρόγραμμα.
xdm-pid	Το ID της διεργασίας του τρέχοντος XDM.

Επίσης σε αυτόν τον κατάλογο υπάρχουν μερικά scripts και προγράμματα που χρησιμοποιούνται για να ρυθμίσουν την επιφάνεια εργασίας όταν εκτελείται το XDM. Θα περιγράψουμε περιληπτικά το σκοπό καθενός από αυτά τα αρχεία. Η ακριβής σύνταξη και χρήση όλων αυτών των αρχείων περιγράφεται στο xdm(1).

Η προκαθορισμένη ρύθμιση είναι ένα απλό ορθογώνιο παράθυρο σύνδεσης με το όνομα του μηχανήματος να φαίνεται στην κορυφή με μεγάλα γράμματα και τις προτροπές "Login:" και "Password:" από κάτω. Αυτό είναι ένα καλό σημείο εκκίνησης για να αλλάξετε την εμφάνιση του XDM.

7.6.3.1. Xaccess

Το πρωτόκολλο για σύνδεση με απεικονίσεις που ελέγχονται από το XDM ονομάζεται X Display Manager Connection Protocol (XDMCP). Το αρχείο αυτό είναι ένα σύνολο κανόνων για των έλεγχο των συνδέσεων XDMCP από απομακρυσμένα μηχανήματα. Αγνοείται, εκτός και αν το xdm-config έχει ρυθμιστεί ώστε να δέχεται εισερχόμενες συνδέσεις. Η προεπιλογή είναι να μην επιτρέπεται σε κανένα πελάτη να συνδεθεί.

7.6.3.2. Xresources

Πρόκειται για το αρχείο προκαθορισμένων τιμών για τις εφαρμογές εμφάνισης του παράθυρου σύνδεσης (login) και επιλογέα απεικόνισης (display chooser). Μέσα από αυτό μπορεί να τροποποιηθεί η εμφάνιση του προγράμματος login. Η μορφή του είναι ίδια με το αρχείο app-defaults που περιγράφεται στην τεκμηρίωση του X11.

7.6.3.3. Xservers

Αυτή είναι μια λίστα των απομακρυσμένων σταθμών που πρέπει να εμφανίζονται ως επιλογές στο πρόγραμμα (chooser).

7.6.3.4. Xsession

Αυτό είναι το προκαθορισμένο session script που εκτελεί το XDM μετά τη σύνδεση κάποιου χρήστη. Κανονικά, κάθε χρήστης θα έχει ένα τροποποιημένο, δικό του, session script στο ~/.xsession που θα παρακάμπτει αυτό το script.

7.6.3.5. Xsetup_*

Τα αρχεία αυτά εκτελούνται αυτόματα πριν την εμφάνιση των παραθύρων επιλογής ή σύνδεσης. Υπάρχει ένα script για κάθε display που χρησιμοποιείται, που ονομάζεται Xsetup_ με το νούμερο του display στο τέλος (για παράδειγμα Xsetup_0). Κανονικά αυτά τα scripts θα εκτελούν ένα ή δυο προγράμματα στο παρασκήνιο όπως π.χ. το `xconsole`.

7.6.3.6. xdm-config

Το αρχείο αυτό περιέχει ρυθμίσεις στην μορφή των app-defaults, που εφαρμόζονται σε κάθε display που διαχειρίζεται η συγκεκριμένη εγκατάσταση.

7.6.3.7. xdm-errors

Το αρχείο αυτό περιέχει την έξοδο των διακομιστών X που προσπαθεί να εκτελέσει το XDM. Αν ένα display που προσπαθεί να εκκινήσει ο XDM κολλήσει για κάποιο λόγο, καλό είναι να αναζητήσετε εδώ τυχόν μηνύματα σφαλμάτων. Τα μηνύματα αυτά καταγράφονται και στα αρχεία χρηστών ~/.xsession-errors.

7.6.4. Διατηρώντας έναν Διακομιστή Απομακρυσμένων Συνδέσεων

Για να συνδέονται και άλλοι πελάτες στον διακομιστή οθόνης, τροποποιήστε τους κανόνες ελέγχου πρόσβασης, και ενεργοποιήστε τις εισερχόμενες συνδέσεις. Τα παραπάνω είναι, από προεπιλογή ρυθμισμένα σε συντηρητικές τιμές. Για να κάνετε το XDM να δέχεται συνδέσεις, αρχικά μετατρέψτε σε σχόλιο την παρακάτω γραμμή στο αρχείο xdm-config:

```
! SECURITY: do not listen for XDMCP or Chooser requests
! Comment out this line if you want to manage X terminals with xdm
DisplayManager.requestPort:     0
```

και μετά επανεκκινήστε τον XDM. Να έχετε υπόψιν σας ότι τα σχόλια στα αρχεία app-defaults

ξεκινούν με τον χαρακτήρα "!", και όχι τον συνήθη "#". Μπορεί να επιθυμείτε πιο αυστηρούς κανόνες ελέγχου πρόσβασης. Δείτε τα παραδείγματα στο Xaccess, και συμβουλευθείτε τη σελίδα manual του xdm(1).

7.6.5. Αντικαταστάτες του XDM

Υπάρχουν αρκετοί αντικαταστάτες για το πρόγραμμα XDM. Ένας από αυτούς, ο KDM (έρχεται με το KDE) αναλύεται αργότερα σε αυτό το κεφάλαιο. Ο KDM display manager προσφέρει πολλά προτερήματα στα γραφικά και διακοσμητικά στοιχεία, όπως επίσης και την δυνατότητα να επιλέγουν οι χρήστες τον επιθυμητό διαχειριστή παραθύρων την στιγμή της σύνδεσης.

7.7. Γραφικά Περιβάλλοντα

Αυτό το τμήμα περιγράφει μερικά γραφικά περιβάλλοντα που διατίθενται για το X στο FreeBSD. Η έννοια "γραφικό περιβάλλον" μπορεί να σημαίνει οτιδήποτε, από έναν απλό διαχειριστή παραθύρων μέχρι ένα ολοκληρωμένα πακέτο desktop εφαρμογών, όπως το KDE ή το GNOME.

7.7.1. GNOME

7.7.1.1. Σχετικά με το GNOME

Το GNOME είναι ένα φιλικό προς τον χρήστη γραφικό περιβάλλον που επιτρέπει στους χρήστες να χρησιμοποιούν και να ρυθμίζουν εύκολα τους υπολογιστές τους. Το GNOME διαθέτει ένα panel (για την εκκίνηση εφαρμογών και την προβολή κατάστασης), επιφάνεια εργασίας (όπου εμφανίζονται δεδομένα και εφαρμογές), ένα πλήθος από διαδεδομένα εργαλεία και εφαρμογές, καθώς και ένα σύνολο τυποποιήσεων που επιτρέπει στις εφαρμογές να συνεργάζονται μεταξύ τους και να δείχνουν ένα συνεπές περιβάλλον εργασίας. Οι χρήστες άλλων λειτουργικών συστημάτων ή περιβάλλοντων θα αισθάνονται σαν στο σπίτι τους χρησιμοποιώντας το πανίσχυρο γραφικό περιβάλλον που παρέχει το GNOME. Περισσότερες πληροφορίες σχετικά με το GNOME στο FreeBSD μπορούν να βρεθούν στο διαδικτυακό τόπο του FreeBSD GNOME Project. Η τοποθεσία περιέχει επίσης και αναλυτικά FAQs σχετικά με την εγκατάσταση, την ρύθμιση, και την διαχείριση του GNOME.

7.7.1.2. Εγκατάσταση του GNOME

Το GNOME μπορεί να εγκατασταθεί εύκολα από πακέτα ή από την Συλλογή των Ports:

Για να εγκαταστήσετε το έτοιμο πακέτο του GNOME από το δίκτυο, απλώς πληκτρολογήστε:

```
# pkg_add -r gnome2
```

Για να μεταγλωττίσετε το GNOME από τον πηγαίο κώδικα, χρησιμοποιήστε την Συλλογή των Ports:

```
# cd /usr/ports/x11/gnome2
# make install clean
```

Το GNOME χρειάζεται το σύστημα αρχείων /proc για να λειτουργήσει σωστά. Προσθέστε τη γραμμή

```
proc           /proc       procfs  rw  0   0
```

στο αρχείο /etc/fstab για να γίνεται αυτόματα προσάρτηση του procfs(5) κατά την εκκίνηση του συστήματος.

Μόλις εγκατασταθεί το GNOME, θα πρέπει να ρυθμιστεί ο διακομιστής X ώστε να εκκινεί το GNOME αντί για τον προκαθορισμένο διαχειριστή παραθύρων.

Ο ευκολότερος τρόπος για να εκκινήσετε το GNOME είναι με το GDM, τον GNOME Display Manager. Το GDM εγκαθίσταται ως μέρος του GNOME, αλλά είναι ανενεργό αρχικά. Μπορεί να ενεργοποιηθεί με την προσθήκη της γραμμής

```
gdm_enable="YES"
```

στο αρχείο /etc/rc.conf.

Μόλις κάνετε επανεκκίνηση, το GDM θα ξεκινήσει αυτόματα.

Επιπρόσθετα, είναι χρήσιμο να ξεκινούν όλες οι υπηρεσίες τις οποίες απαιτεί το GNOME ταυτόχρονα με την εκκίνηση του GDM. Για να γίνεται αυτό προσθέστε τη γραμμή

```
gnome_enable="YES"
```

στο αρχείο /etc/rc.conf.

Το GNOME μπορεί επίσης να ξεκινήσει από την γραμμή εντολών ρυθμίζοντας κατάλληλα το αρχείο .xinitrc. Αν υπάρχει ήδη το αρχείο .xinitrc, απλώς αντικαταστήστε την γραμμή που εκκινεί τον τρέχοντα διαχειριστή παραθύρων με μία που να εκκινεί το /usr/local/bin/gnome-session. Αν δεν θέλετε να κάνετε περισσότερες ρυθμίσεις στο αρχείο, χρειάζεται απλά να γράψετε:

```
% echo "/usr/local/bin/gnome-session" > ~/.xinitrc
```

Έπειτα, πληκτρολογήστε `startx`, και θα ξεκινήσει το γραφικό περιβάλλον του GNOME

Αν χρησιμοποιείτε κάποιο παλαιότερο display manager, όπως το XDM, το παραπάνω δεν θα λειτουργήσει. Στην περίπτωση αυτή, δημιουργήστε ένα εκτελέσιμο αρχείο .xsession το οποίο να περιέχει την ίδια εντολή. Τροποποιήστε το αρχείο .xsession και αντικαταστήστε την εντολή του τρέχοντος διαχειριστή παραθύρων με το /usr/local/bin/gnome-session:

```
% echo "#!/bin/sh" > ~/.xsession
% echo "/usr/local/bin/gnome-session" >> ~/.xsession
% chmod +x ~/.xsession
```

Άλλη μια επιλογή είναι να ρυθμιστεί ο display manager ώστε να επιτρέπει την επιλογή του διαχειριστή παραθύρων κατά την σύνδεση. Το τμήμα Λεπτομέρειες KDE εξηγεί πως μπορεί να γίνει αυτό μέσω του KDM, του display manager του KDE.

7.7.2. KDE

7.7.2.1. Σχετικά με το KDE

Το KDE είναι ένα σύγχρονο, εύκολο στη χρήση, γραφικό περιβάλλον. Μερικά πράγματα που προσφέρει το KDE στον χρήστη είναι:

- Ένα όμορφο σύγχρονο περιβάλλον
- Ένα περιβάλλον με πλήρη δικτυακή διαφάνεια
- Ένα ενσωματωμένο σύστημα βοήθειας που επιτρέπει εύκολη, συνεπή πρόσβαση στην βοήθεια για την χρήση του KDE και των εφαρμογών του
- Συνεπής εμφάνιση και συμπεριφορά όλων των εφαρμογών του KDE
- Τυποποιημένα menu και γραμμές εργαλείων (toolbars), συνδυασμοί πλήκτρων, χρωματικοί συνδυασμοί, κλπ.
- Διεθνείς ρυθμίσεις: το KDE διατίθεται σε περισσότερες από 55 γλώσσες
- Κεντρικό και συνεπές σύστημα ρυθμίσεων βασισμένο σε διαλόγους
- Μεγάλο αριθμό χρήσιμων εφαρμογών, σχεδιασμένων ειδικά για το KDE

Το KDE συνοδεύεται από έναν περιηγητή (browser) που ονομάζεται Konqueror, και ανταγωνίζεται σοβαρά τους άλλους περιηγητές των συστημάτων UNIX®. Περισσότερες πληροφορίες για το KDE μπορείτε να βρείτε στο KDE website. Για πληροφορίες σχετικές με το FreeBSD και το KDE, συμβουλευθείτε τον διαδικτυακό τόπο του KDE/FreeBSD.

Υπάρχουν διαθέσιμες δύο εκδόσεις του KDE για το FreeBSD. Η Έκδοση 3, κυκλοφορεί αρκετό καιρό και είναι ακόμα διαθέσιμη στη Συλλογή των Ports αν και δεν συντηρείται πλέον και παρουσιάζει προβλήματα. Η έκδοση 4 ανανεώνεται συνεχώς και είναι η προεπιλογή των χρηστών του KDE. Οι δύο αυτές εκδόσεις μπορούν κάλιστα να συνυπάρχουν στον ίδιο υπολογιστή.

7.7.2.2. Εγκατάσταση του KDE

Όπως και με το GNOME ή κάθε άλλο γραφικό περιβάλλον, το λογισμικό μπορεί να εγκατασταθεί εύκολα μέσω πακέτων ή από την Συλλογή των Ports:

Για να εγκαταστήσετε το KDE 3 μέσω πακέτων από το δίκτυο, απλώς πληκτρολογήστε:

```
# pkg_add -r kde
```

Για να εγκαταστήσετε το KDE 4 μέσω πακέτων από το δίκτυο, απλώς πληκτρολογήστε:

```
# pkg_add -r kde4
```

Το pkg_add(1) θα ανακτήσει αυτόματα την τελευταία έκδοση της εφαρμογής.

Για να μεταγλωττίσετε το KDE 3 από τον πηγαίο κώδικα, χρησιμοποιήστε τη Συλλογή των Ports:

```
# cd /usr/ports/x11/kde3
# make install clean
```

Για να μεταγλωττίσετε το KDE 4 από τον πηγαίο κώδικα, χρησιμοποιήστε τη Συλλογή των Ports:

```
# cd /usr/ports/x11/kde4
# make install clean
```

Αφού εγκατασταθεί το KDE, θα πρέπει να ρυθμιστεί ο διακομιστής X ώστε να το εκκινεί αντί για τον προκαθορισμένο διαχειριστή παραθύρων. Αυτό γίνεται με την αλλαγή του αρχείου .xinitrc:

Για το KDE 3:

```
% echo "exec startkde" > ~/.xinitrc
```

Για το KDE 4:

```
% echo "exec /usr/local/kde4/bin/startkde" > ~/.xinitrc
```

Τώρα, όποτε το X Window System εκκινείται μέσω του `startx`, το γραφικό περιβάλλον θα είναι το KDE.

Αν χρησιμοποιείτε κάποιο display manager όπως το XDM, η ρύθμιση είναι λίγο διαφορετική. Θα πρέπει αντί για το .xinitrc να τροποποιήσετε το .xsession. Οδηγίες για το KDM δίνονται αργότερα στο κεφάλαιο αυτό.

7.7.3. Περισσότερες Λεπτομέρειες για το KDE

Τώρα που το KDE έχει εγκατασταθεί στο σύστημα, μπορείτε να ανακαλύψετε τις περισσότερες λειτουργίες μέσω των σελίδων βοήθειας ή δοκιμάζοντας μενού και επιλογές. Οι χρήστες των Windows® η του Mac® θα αισθάνονται σαν στο σπίτι τους.

Η καλύτερη βοήθεια για το KDE είναι η on-line τεκμηρίωση. Το KDE συνοδεύεται από τον δικό του περιηγητή, τον Konqueror, πολλές χρήσιμες εφαρμογές, και αναλυτική τεκμηρίωση. Το υπόλοιπο αυτής της ενότητας συζητά τεχνικά θέματα που είναι δύσκολο να ανακαλυφθούν με δοκιμές.

7.7.3.1. Ο KDE Display Manager

Ο διαχειριστής ενός πολυχρηστικού συστήματος θέλει ενδεχομένως η σύνδεση των χρηστών να γίνεται μέσω γραφικού περιβάλλοντος. Όπως περιγράψαμε πρίν, μπορεί να χρησιμοποιηθεί το XDM. Όμως, το KDE περιέχει μια εναλλακτική επιλογή, το KDM, το οποίο έχει σχεδιαστεί να είναι ποίο ελκυστικό και παρέχει περισσότερες επιλογές κατά τη σύνδεση. Συγκεκριμένα, οι χρήστες μπορούν

εύκολα να επιλέξουν (μέσω μενού) ποίο γραφικό περιβάλλον (KDE, GNOME, ή κάποιο άλλο) θα εκτελεστεί μετά την σύνδεση τους.

Για να ενεργοποιήσετε το KDM, θα πρέπει να επεξεργαστείτε κάποια αρχεία, τα οποία είναι διαφορετικά ανάλογα με την έκδοση του KDE που θα χρησιμοποιήσετε.

Για το KDE 3, θα πρέπει να τροποποιήσετε την εγγραφή για το `ttyv8` στο /etc/ttys, όπως φαίνεται παρακάτω:

```
ttyv8 "/usr/local/bin/kdm -nodaemon" xterm on secure
```

Για το KDE 4, θα πρέπει να προσαρτήσετε το procfs(5) και να προσθέσετε την παρακάτω γραμμή στο /etc/rc.conf:

```
kdm4_enable="YES"
```

7.7.4. Xfce

7.7.4.1. Σχετικά με το Xfce

Το Xfce είναι ένα γραφικό περιβάλλον που στηρίζεται στην βιβλιοθήκη GTK+ που χρησιμοποιείται και από το GNOME, αλλά είναι πολύ πιο ελαφρύ και προορίζεται για όσους θέλουν ένα απλό, αποτελεσματικό γραφικό περιβάλλον που είναι εύκολο να χρησιμοποιηθεί και να ρυθμιστεί. Οπτικά, μοιάζει πολύ με το CDE, που συναντάται σε εμπορικά συστήματα UNIX®. Μερικά από τα χαρακτηριστικά του Xfce είναι:

- Ένα απλό, εύκολο στην χρήση γραφικό περιβάλλον
- Πλήρως παραμετροποιήσιμο με το ποντίκι, με drag and drop, κλπ.
- Κεντρικό panel παρόμοιο με του CDE, με μενού, μικρο-εφαρμογές και πλήκτρα εκκίνησης εφαρμογών
- Ολοκληρωμένος διαχειριστής παραθύρων, διαχειριστής αρχείων, διαχειριστής ήχου, συμβατότητα με το GNOME, και άλλα
- Δυνατότητα χρήσης θεμάτων (themes, αφού χρησιμοποιεί το GTK+)
- Γρήγορο, ελαφρύ και αποτελεσματικό: ιδανικό για παλαιότερα/πιο αργά μηχανήματα ή μηχανήματα με λίγη μνήμη

Περισσότερες πληροφορίες για το Xfce μπορείτε να βρείτε στη δικτυακή τοποθεσία του Xfce.

7.7.4.2. Εγκατάσταση του Xfce

Υπάρχει (την ώρα που γράφονται αυτές οι γραμμές) έτοιμο πακέτο για το Xfce. Για να το εγκαταστήσετε, απλώς πληκτρολογήστε:

```
# pkg_add -r xfce4
```

Εναλλακτικά, για να το μεταγλωττίσετε από τον πηγαίο κώδικα, χρησιμοποιήστε την Συλλογή των Ports:

```
# cd /usr/ports/x11-wm/xfce4
# make install clean
```

Τώρα, πείτε στον διακομιστή X να εκκινήσει το Xfce την επόμενη φορά που θα γίνει εκκίνηση του γραφικού περιβάλλοντος. Απλώς πληκτρολογήστε το παρακάτω:

```
% echo "/usr/local/bin/startxfce4" > ~/.xinitrc
```

Την επόμενη φορά που θα εκκινήσετε το X, θα εμφανιστεί το Xfce. Όπως και προηγουμένως, αν χρησιμοποιείτε κάποιο display manager όπως το XDM, δημιουργήστε ένα αρχείο .xsession, όπως περιγράφεται στην παράγραφο του GNOME, αλλά με την εντολή /usr/local/bin/startxfce4, ή ρυθμίστε τον display manager να επιτρέπει την επιλογή γραφικού περιβάλλοντος, όπως περιγράφεται στην παράγραφο σχετικά με το kdm.

params: path: "/books/handbook/partii/" :leveloffset: +1

Part II: Desktop Εφαρμογές

Chapter 8. Σύνοψη

Το FreeBSD μπορεί να εκτελέσει μια ευρεία γκάμα desktop εφαρμογών, όπως φυλλομετρητές (browsers) και επεξεργαστές κειμένου. Οι περισσότερες από αυτές είναι διαθέσιμες ως πακέτα (packages) ή μπορούν να εγκατασταθούν αυτόματα από την Συλλογή των Ports. Πολλοί νέοι χρήστες αναμένουν να βρουν τέτοιου είδους εφαρμογές στο desktop τους. Το κεφάλαιο αυτό θα σας δείξει πως να εγκαταστήσετε χωρίς κόπο τις πιο δημοφιλείς desktop εφαρμογές, είτε από πακέτα είτε από τη Συλλογή των Ports.

Σημειώστε ότι όταν εγκαθιστάτε προγράμματα από τη Συλλογή των Ports, γίνεται μεταγλώττιση από τον πηγαίο κώδικα. Αυτό μπορεί να χρειαστεί πολύ χρόνο, καθώς εξαρτάται από το πρόγραμμα το οποίο μεταγλωττίζετε και την υπολογιστική ισχύ του μηχανήματός σας. Αν το χρονικό διάστημα το οποίο χρειάζεται η μεταγλώττιση είναι απαγορευτικά μεγάλο, μπορείτε να εγκαταστήσετε τα περισσότερα προγράμματα της Συλλογής των Ports από προ-μεταγλωττισμένα πακέτα.

Καθώς το FreeBSD διαθέτει συμβατότητα με εκτελέσιμα προγράμματα για Linux, πολλές εφαρμογές που αναπτύχθηκαν αρχικά για το Linux είναι διαθέσιμες για το desktop σας. Σας συνιστούμε θερμά να διαβάσετε το Συμβατότητα με Εκτελέσιμα του Linux πριν εγκαταστήσετε οποιαδήποτε από τις εφαρμογές Linux. Πολλά από τα ports που χρησιμοποιούν τη συμβατότητα με Linux έχουν ονόματα που ξεκινούν με "linux-". Θυμηθείτε το όταν ψάχνετε για κάποιο συγκεκριμένο port, για παράδειγμα με την whereis(1). Στο κείμενο που ακολουθεί θεωρείται ότι έχετε ενεργοποιήσει την συμβατότητα με εκτελέσιμα προγράμματα Linux πριν εγκαταστήσετε οποιαδήποτε από τις εφαρμογές του Linux.

Οι κατηγορίες που καλύπτονται από αυτό το κεφάλαιο είναι οι εξής:

- Φυλλομετρητές (όπως Firefox, Opera, KonquerorChromium)
- Εφαρμογές γραφείου (όπως KOffice, AbiWord, The GIMP, OpenOffice.org, LibreOffice)
- Προγράμματα προβολής εγγράφων (όπως Acrobat Reader®, gv, Xpdf, GQview)
- Χρηματοοικονομικές εφαρμογές (όπως GnuCash, Gnumeric, Abacus)

Πριν διαβάσετε αυτό το κεφάλαιο θα πρέπει:

- Να ξέρετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).
- Να ξέρετε πως να εγκαταστήσετε πρόσθετο λογισμικό Linux (Συμβατότητα με Εκτελέσιμα του Linux).

Για πληροφορίες σχετικά με την εγκατάσταση πολυμεσικού περιβάλλοντος διαβάστε το Πολυμέσα. Αν θέλετε να ρυθμίσετε και να χρησιμοποιήσετε κάποια υπηρεσία ηλεκτρονικού ταχυδρομείου δείτε το Ηλεκτρονικό Ταχυδρομείο.

Chapter 9. Φυλλομετρητές (Browsers)

Το FreeBSD δεν έχει προεγκατεστημένο κάποιο συγκεκριμένο φυλλομετρητή. Στον κατάλογο www της συλλογής Ports μπορείτε να βρείτε αρκετούς φυλλομετρητές, έτοιμους για εγκατάσταση. Αν δεν έχετε χρόνο για να μεταγλωττίσετε ότι χρειάζεστε (ίσως χρειαστείτε αρκετή ώρα), πολλοί από αυτούς είναι διαθέσιμοι και ως έτοιμα πακέτα.

Τα KDE και GNOME, ως πλήρη περιβάλλοντα εργασίας, παρέχουν τους δικούς τους φυλλομετρητές HTML. Δείτε το Γραφικά Περιβάλλοντα για περισσότερες πληροφορίες σχετικά με την εγκατάσταση τους.

Αν ενδιαφέρεστε για ελαφρείς (από άποψη κατανάλωσης πόρων) φυλλομετρητές, δείτε τις ακόλουθες εφαρμογές στη συλλογή των Ports: www/dillo2, www/links, ή www/w3m.

Το τμήμα αυτό καλύπτει τις παρακάτω εφαρμογές:

Όνομα Εφαρμογής	Άδεια	Πακέτο	Απαιτούμενοι Πόροι
Firefox	MPL 2.0	www/firefox	βαριά
Chromium	BSD-3	www/chromium	βαριά
Iridium browser	BSD-3	www/iridium-browser	βαριά
Falkon	MPL 2.0	www/falkon-qtonly	βαριά
Konqueror	GPL 2.0 ή νεότερη	x11-fm/konqueror	μεσαία
Gnome Web (Epiphany)	GPL 3.0 ή νεότερη	www/epiphany	μεσαία
qutebrowser	GPL 3.0 ή νεότερη	www/qutebrowser	μεσαία
Dillo	GPL 3.0 ή νεότερη	www/dillo	ελαφριά
Links	GPL 2.0 ή νεότερη	www/links	ελαφριά
w3m	MIT	www/w3m	ελαφριά

9.1. Firefox

Ο Firefox είναι ένας μοντέρνος, ελεύθερος, ανοιχτός και σταθερός φυλλομετρητής, ο οποίος είναι πλήρως προσαρμοσμένος για χρήση στο FreeBSD. Διαθέτει μηχανή απεικόνισης η οποία εναρμονίζεται πλήρως με τις τυποποιήσεις της HTML, και δυνατότητες όπως εμφάνιση πολλαπλών σελίδων σε tabs, μπλοκάρισμα αναδυόμενων παραθύρων (popups), πρόσθετα προγράμματα, βελτιωμένη ασφάλεια και πολλά ακόμη. Ο Firefox βασίζεται στον αρχικό πηγαίο κώδικα του Mozilla.

Εγκαταστήστε το πακέτο γράφοντας:

```
# pkg install firefox
```

Η παραπάνω εντολή θα εγκαταστήσει την τελευταία σταθερή έκδοση του Firefox. Αν θέλετε να εγκαταστήσετε την παλιά έκδοση εκτεταμένης υποστήριξης (Extended Support Release, ESR), πληκτρολογήστε:

```
# pkg install firefox-esr
```

Μπορείτε επίσης να χρησιμοποιήσετε την Συλλογή των Ports αν προτιμάτε να μεταγλωττίσετε από τον πηγαίο κώδικα:

```
# cd /usr/ports/www/firefox
# make install clean
```

Για τον Firefox ESR, αντικαταστήστε στην παραπάνω εντολή τη λέξη `firefox` με `firefox-esr`.

9.2. Opera

Ο Opera είναι ένας φυλλομετρητής με πλήρεις δυνατότητες και συμβατός με τα πρότυπα. Έρχεται επίσης με ενσωματωμένο πρόγραμμα ανάγνωσης ταχυδρομείου (mail) και ειδήσεων (news), πρόγραμμα για IRC, αναγνώστη για RSS/Atom και πολλά ακόμα. Παρ'όλα αυτά, ο Opera είναι μια σχετικά ελαφριά και πολύ γρήγορη εφαρμογή. Έρχεται σε δύο τύπους: μια "εγγενής" έκδοση για το FreeBSD και μια έκδοση που εκτελείται μέσω της συμβατότητας με το Linux.

Για να χρησιμοποιήσετε την FreeBSD έκδοση του Opera, εγκαταστήστε το πακέτο:

```
# pkg_add -r opera
```

Ορισμένες τοποθεσίες FTP δεν διαθέτουν όλα τα πακέτα, αλλά μπορείτε να έχετε το ίδιο αποτέλεσμα μέσω της συλλογής των Ports, γράφοντας:

```
# cd /usr/ports/www/opera
# make install clean
```

Για να εγκαταστήσετε την Linux έκδοση του Opera, αντικαταστήστε με `linux-opera` το `opera` στα παραπάνω παραδείγματα.

Το πρόσθετο Adobe® Flash™ δεν είναι διαθέσιμο για το FreeBSD. Διατίθεται ωστόσο μια έκδοση κατάλληλη για το Linux®. Για να την χρησιμοποιήσετε θα πρέπει αρχικά να εγκαταστήσετε το port www/linux-f10-flashplugin11 και έπειτα το port www/opera-linuxplugins:

```
# cd /usr/ports/www/linux-f11-flashplugin10
# make install clean
# cd /usr/ports/www/opera-linuxplugins
# make install clean
```

Μπορείτε να ελέγξετε εύκολα την ύπαρξη του plugin: ξεκινήστε τον φυλλομετρητή σας, γράψτε `opera:plugins` στη γραμμή διευθύνσεων και πιέστε `Enter`. Θα πρέπει να δείτε μια λίστα με όλα τα διαθέσιμα πρόσθετα.

Για να προσθέσετε το πρόσθετο της Java™, ακολουθήστε τις αντίστοιχες οδηγίες για τον Firefox.

9.3. Konqueror

Ο Konqueror είναι κομμάτι του KDE αλλά μπορεί να χρησιμοποιηθεί και έξω από το KDE με την εγκατάσταση του x11/kdebase3. Ο Konqueror είναι πολύ περισσότερο από ένας απλός φυλλομετρητής, είναι επίσης διαχειριστής αρχείων και πρόγραμμα προβολής αρχείων πολυμέσων.

Ο Konqueror διατίθεται επίσης με ένα σετ από plugins, στο misc/konq-plugins.

Ο Konqueror υποστηρίζει τόσο το WebKit όσο και το δικό του KHTML. Το WebKit χρησιμοποιείται από πολλούς σύγχρονους φυλλομετρητές, συμπεριλαμβανομένου και του Chromium. Για να χρησιμοποιήσετε το WebKit με τον Konqueror στο FreeBSD:

```
# cd /usr/ports/www/kwebkitpart
# make install clean
```

Μετά την εγκατάσταση, στον Konqueror κάντε κλικ στο "Settings", "Configure Konqueror" και τέλος στο "Change KHTML to WebKit".

Ο Konqueror υποστηρίζει επίσης Flash™ και οι σχετικές οδηγίες (How To) είναι διαθέσιμες στο http://freebsd.kde.org/howtos/konqueror-flash.php.

9.4. Chromium

Ο Chromium είναι μια εφαρμογή browser ανοικτού κώδικα που στοχεύει στη βελτίωση της εμπειρίας του χρήστη παρέχοντας ένα φυλλομετρητή ο οποίος είναι ασφαλέστερος, ταχύτερος και πιο σταθερός. Ο Chromium παρέχει δυνατότητα εμφάνισης σελίδων σε καρτέλες, αποκλεισμό αναδυόμενων παραθύρων (popup blocker), πρόσθετα (extensions) και πολλά ακόμα. Ο Chromium είναι το Έργο ανοικτού κώδικα στο οποίο βασίζεται ο φυλλομετρητής Google Chrome.

Ο Chromium μπορεί να εγκατασταθεί από πακέτο, με την εντολή:

```
# pkg_add -r chromium
```

Εναλλακτικά, μπορείτε να μεταγλωττίσετε τον Chromium χρησιμοποιώντας τη Συλλογή των Ports:

```
# cd /usr/ports/www/chromium
# make install clean
```

Ο Chromium εγκαθιστάται ως /usr/local/bin/chrome και όχι ως /usr/local/bin/chromium.

9.5. Ο Chromium και το Πρόσθετο της Java™

Στην ενότητα αυτή θεωρούμε ότι έχετε ήδη εγκαταστήσει τον Chromium.

Εγκαταστήστε το OpenJDK 6 μέσω της Συλλογής των Ports, γράφοντας:

```
# cd /usr/ports/java/openjdk6
# make install clean
```

Έπειτα, εγκαταστήστε το java/icedtea-web από τη Συλλογή των Ports:

```
# cd /usr/ports/java/icedtea-web
# make install clean
```

Ξεκινήστε τον Chromium και πληκτρολογήστε `about:plugins` στη γραμμή διευθύνσεων. Θα πρέπει να δείτε το IcedTea-Web να εμφανίζεται ως ένα από τα πρόσθετα.

Αν το πρόσθετο δεν εμφανίζεται στον Chromium, εκτελέστε τις παρακάτω εντολές και επανεκκινήστε το φυλλομετρητή σας:

```
# mkdir -p /usr/local/shared/chromium/plugins
#  ln -s /usr/local/lib/IcedTeaPlugin.so \
  /usr/local/shared/chromium/plugins/
```

9.6. Ο Chromium και το Πρόσθετο Adobe® Flash™

Στην ενότητα αυτή θεωρούμε ότι έχετε ήδη εγκαταστήσει τον Chromium.

Για τη ρύθμιση του Chromium για χρήση με το πρόσθετο Adobe® Flash™, χρησιμοποιήστε τις οδηγίες για τον Firefox. Στον προηγούμενο σύνδεσμο θα βρείτε πλήρεις οδηγίες για την εγκατάσταση του Adobe® Flash™ στο FreeBSD. Δεν απαιτούνται επιπλέον βήματα, καθώς ο Chromium μπορεί να χρησιμοποιήσει κάποια πρόσθετα από άλλους φυλλομετρητές.

Chapter 10. Εφαρμογές Γραφείου

Όσο αφορά τις εφαρμογές γραφείου, οι νέοι χρήστες συχνά αναζητούν μια καλή σουίτα εφαρμογών ή ένα φιλικό επεξεργαστή κειμένου. Αν και κάποια γραφικά περιβάλλοντα όπως το KDE παρέχουν τη δική τους σουίτα εφαρμογών γραφείου, δεν υπάρχει ωστόσο προεπιλεγμένη εφαρμογή. Το FreeBSD παρέχει ότι χρειάζεστε, άσχετα από το περιβάλλον εργασίας σας.

Το τμήμα αυτό καλύπτει τις παρακάτω εφαρμογές:

Όνομα Εφαρμογής	Απαιτούμενοι Πόροι	Εγκατάσταση από Ports	Βασικές Εξαρτήσεις
KOffice	λίγοι (ελαφριά)	βαριά	KDE
AbiWord	λίγοι (ελαφριά)	ελαφριά	Gtk+ ή GNOME
The Gimp	λίγοι (ελαφριά)	βαριά	Gtk+
OpenOffice.org	πολλοί (βαριά)	εξαιρετικά βαριά	JDK™, Mozilla
LibreOffice	σχετικά βαριά	τεράστια	Gtk+ ή KDE/ GNOME ή JDK™

10.1. KOffice

Η κοινότητα του KDE εξοπλίζει το γραφικό της περιβάλλον με μια σουίτα εφαρμογών γραφείου που μπορεί να χρησιμοποιηθεί και έξω από το KDE. Περιλαμβάνει τα τέσσερα βασικά προγράμματα που μπορείτε επίσης να βρείτε και σε άλλες σουίτες γραφείου. Το KWord είναι ο επεξεργαστής κειμένου, το KSpread είναι το πρόγραμμα υπολογιστικών φύλλων, το KPresenter διαχειρίζεται τις παρουσιάσεις, ενώ το Kontour σας επιτρέπει να δημιουργήσετε έγγραφα με γραφικά.

Πριν εγκαταστήσετε το τελευταίο KOffice, βεβαιωθείτε ότι έχετε ανανεωμένη έκδοση του KDE.

Για να εγκαταστήσετε το KOffice για το KDE4 ως πακέτο, δώστε την ακόλουθη εντολή:

```
# pkg_add -r koffice-kde4
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports. Για παράδειγμα, για να εγκαταστήσετε το KOffice για το KDE4, πληκτρολογήστε:

```
# cd /usr/ports/editors/koffice-kde4
# make install clean
```

10.2. AbiWord

Το AbiWord είναι ένα ελεύθερο πρόγραμμα επεξεργασίας κειμένου, όμοιο στην αίσθηση και την εμφάνιση με το Microsoft® Word. Είναι κατάλληλο για την πληκτρολόγηση άρθρων, γραμμάτων, αναφορών, υπενθυμίσεων κ.ο.κ. Είναι πολύ γρήγορο, έχει αρκετές δυνατότητες και είναι ιδιαίτερα

φιλικό στο χρήστη.

Το AbiWord μπορεί να εισάγει ή να εξάγει αρχεία διάφορων μορφών, περιλαμβανομένων και κάποιων κλειστών όπως το .doc της Microsoft®.

Το AbiWord είναι διαθέσιμο ως πακέτο. Μπορείτε να το εγκαταστήσετε γράφοντας:

```
# pkg_add -r abiword
```

Αν το πακέτο δεν είναι διαθέσιμο για κάποιο λόγο, μπορείτε να το μεταγλωττίσετε από την Συλλογή των Ports. Σε αυτή την περίπτωση πιθανώς να εγκαταστήσετε νεώτερη έκδοση σε σχέση με το έτοιμο πακέτο. Μπορείτε να το κάνετε ως εξής:

```
# cd /usr/ports/editors/abiword
# make install clean
```

10.3. Το GIMP

Το The GIMP είναι ένα ιδιαίτερα εξελιγμένο πρόγραμμα διαχείρισης γραφικών για δημιουργία εικόνων ή επεξεργασία φωτογραφιών. Μπορεί να χρησιμοποιηθεί ως απλό πρόγραμμα ζωγραφικής ή σαν σουίτα επεξεργασίας και διόρθωσης φωτογραφιών. Περιέχει μεγάλο αριθμό από plugins ενώ διαθέτει και scripting interface. Το The GIMP μπορεί να διαβάσει και να γράψει μεγάλο φάσμα αρχείων εικόνας. Περιλαμβάνει επίσης διεπαφές διασύνδεσης με σαρωτές και tablets.

Μπορείτε να εγκαταστήσετε το πακέτο δίνοντας την εντολή:

```
# pkg_add -r gimp
```

Αν η τοποθεσία FTP που χρησιμοποιείτε δεν διαθέτει αυτό το πακέτο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports. Ο κατάλογος graphics της Συλλογής των Ports περιέχει επίσης και το The Gimp Manual (εγχειρίδιο χρήσης). Δείτε παρακάτω πως να το εγκαταστήσετε:

```
# cd /usr/ports/graphics/gimp
# make install clean
# cd /usr/ports/graphics/gimp-manual-pdf
# make install clean
```

Ο κατάλογος graphics της συλλογής των Ports έχει επίσης την υπό εξέλιξη έκδοση της εφαρμογής The GIMP στο graphics/gimp-devel. Μπορείτε να βρείτε την HTML έκδοση του εγχειριδίου, The Gimp Manual στο graphics/gimp-manual-html.

10.4. OpenOffice.org

Το OpenOffice.org περιέχει όλες τις απαραίτητες εφαρμογές σε μια πλήρη σουίτα εφαρμογών

γραφείου: επεξεργαστή κειμένου, υπολογιστικό φύλλο, διαχειριστή παρουσιάσεων και πρόγραμμα σχεδίασης. Το περιβάλλον εργασίας του είναι πολύ όμοιο με άλλες σουίτες γραφείου, και μπορεί να χρησιμοποιήσει διάφορους δημοφιλείς τύπους αρχείων. Είναι διαθέσιμο σε πολλές διαφορετικές γλώσσες, τόσο ως προς το περιβάλλον εργασίας όσο και ως προς τα λεξικά και τον ορθογραφικό έλεγχο.

Ο επεξεργαστής κειμένου του OpenOffice.org χρησιμοποιεί εγγενώς μορφή αρχείου XML για αυξημένη φορητότητα και ευελιξία. Το πρόγραμμα υπολογιστικών φύλλων διαθέτει γλώσσα μακροεντολών και μπορεί να διασυνδεθεί με εξωτερικές βάσεις δεδομένων. Το OpenOffice.org είναι σταθερή εφαρμογή και εκτελείται εγγενώς στα Windows®, το Solaris™, το Linux, το FreeBSD, καθώς και στο Mac OS® X. Περισσότερες πληροφορίες για το OpenOffice.org μπορείτε να βρείτε στη δικτυακή τοποθεσία του OpenOffice.org. Για πληροφορίες σχετικά με την έκδοση για FreeBSD, καθώς και για απευθείας κατέβασμα πακέτων, χρησιμοποιήστε την δικτυακή τοποθεσία FreeBSD OpenOffice.org Porting Team.

Για να εγκαταστήσετε το OpenOffice.org, γράψτε:

```
# pkg_add -r openoffice.org
```

Αν χρησιμοποιείτε -RELEASE έκδοση του FreeBSD, το παραπάνω πρέπει να δουλέψει. Διαφορετικά, θα πρέπει να δείτε την δικτυακή τοποθεσία του FreeBSD OpenOffice.org Porting Team για να κατεβάσετε και να εγκαταστήσετε το αντίστοιχο πακέτο χρησιμοποιώντας την pkg_add(1). Τόσο η τρέχουσα όσο και η υπό εξέλιξη έκδοση είναι διαθέσιμες για κατέβασμα από την παραπάνω τοποθεσία.

Από τη στιγμή που το πακέτο εγκατασταθεί, πρέπει να γράψετε απλώς την παρακάτω εντολή για να εκτελέσετε το OpenOffice.org:

```
% openoffice.org
```

Κατά την πρώτη εκκίνηση, θα σας γίνουν διάφορες ερωτήσεις και θα δημιουργηθεί ένας κατάλογος με όνομα .openoffice.org μέσα στον προσωπικό σας κατάλογο.

Αν τα πακέτα του OpenOffice.org δεν είναι διαθέσιμα, έχετε πάντα την επιλογή να μεταγλωττίσετε το αντίστοιχο port. Ωστόσο, να έχετε υπόψη σας ότι αυτό απαιτεί αρκετό χώρο στο δίσκο και θα χρειαστεί και πάρα πολύ χρόνο για να ολοκληρωθεί.

```
# cd /usr/ports/editors/openoffice.org-3
# make install clean
```

Αν θέλετε να δημιουργήσετε μια έκδοση με τις δικές σας τοπικές ρυθμίσεις, αντικαταστήστε την προηγούμενη γραμμή εντολών με την επόμενη:

```
# make LOCALIZED_LANG=your_language install clean
```

> Πρέπει να αντικαταστήσετε το *your_language* με το σωστό ISO κωδικό για τη γλώσσα σας. Η λίστα με τους υποστηριζόμενους κωδικούς γλωσσών είναι διαθέσιμη στο αρχείο files/Makefile.localized, το οποίο βρίσκεται στον κατάλογο του port.

Μόλις γίνει αυτό, μπορείτε να ξεκινήσετε την εφαρμογή OpenOffice.org δίνοντας την εντολή:

```
% openoffice.org
```

10.5. LibreOffice

Το LibreOffice είναι μια ελεύθερη σουίτα εφαρμογών γραφείου η οποία αναπτύσσεται από το The Document Foundation. Είναι συμβατή με τις άλλες γνωστές σουίτες γραφείου και διατίθεται για τις περισσότερες πλατφόρμες. Πρόκειται για fork της γνωστής εφαρμογής OpenOffice.org η οποία περιλαμβάνει όλα τα απαραίτητα μιας σουίτας γραφείου: επεξεργαστή κειμένου, υπολογιστικό φύλλο, πρόγραμμα παρουσιάσεων, πρόγραμμα σχεδίασης και ένα εργαλείο για δημιουργία και επεξεργασία μαθηματικών τύπων. Διατίθεται σε πλήθος γλωσσών - η διεθνής υποστήριξη επεκτείνεται μάλιστα τόσο στο περιβάλλον όσο και στα επιπλέον προγράμματα ελέγχου ορθογραφίας και λεξικών.

Ο επεξεργαστής κειμένου του OpenOffice χρησιμοποιεί εγγενώς μορφή αρχείου XML το οποίο εξασφαλίζει αυξημένη φορητότητα και ευελιξία. Το υπολογιστικό φύλλο διαθέτει μια γλώσσα μακροεντολών και μπορεί να διασυνδεθεί με εξωτερικές βάσεις δεδομένων. Το LibreOffice είναι ήδη σταθερό και διατίθεται σε εκδόσεις για Windows®, Linux®, FreeBSD και Mac OS® X. Για περισσότερες πληροφορίες σχετικά με το LibreOffice επισκεφθείτε την δικτυακή τοποθεσία του.

Για να εγκαταστήσετε το LibreOffice από έτοιμο πακετό, γράψτε:

```
# pkg_add -r libreoffice
```

> Το παραπάνω θα λειτουργήσει αν τρέχετε κάποιο επίσημο -RELEASE του FreeBSD.

Μετά την εγκατάσταση του πακέτου, πληκτρολογήστε το παρακάτω για να εκτελέσετε το LibreOffice:

```
% libreoffice
```

> Κατά την πρώτη εκκίνηση, θα σας γίνουν κάποιες ερωτήσεις και θα δημιουργηθεί ένας κατάλογος .libreoffice μέσα στον προσωπικό σας κατάλογο.

Αν δεν υπάρχουν διαθέσιμα πακέτα για το LibreOffice, έχετε επίσης την επιλογή να το μεταγλωττίσετε από το αντίστοιχο port. Θα πρέπει ωστόσο να γνωρίζετε ότι απαιτείται αρκετός χώρος στο δίσκο και αρκετός χρόνος για τη μεταγλώττιση.

```
# cd /usr/ports/editors/libreoffice
# make install clean
```

Αν θέλετε να δημιουργήσετε μια έκδοση με υποστήριξη κάποιας συγκεκριμένης γλώσσας, αντικαταστήστε την προηγούμενη εντολή με:

```
# make LOCALIZED_LANG=your_language install clean
```

Θα πρέπει να αντικαταστήσετε το *your_language* με το σωστό ISO κωδικό της γλώσσας που επιθυμείτε να χρησιμοποιήσετε. Για να βρείτε τον κωδικό, δείτε το αρχείο Makefile του port και ειδικότερα την ενότητα `pre-fetch`.

Μπορείτε έπειτα να εκτελέσετε το LibreOffice χρησιμοποιώντας την παρακάτω εντολή:

```
% libreoffice
```

Chapter 11. Προγράμματα Προβολής Εγγράφων

Πρόσφατα έχουν γίνει αρκετά δημοφιλείς κάποιες νέες μορφές αρχείων. Τα προγράμματα προβολής που απαιτούνται για τα αρχεία αυτά ίσως να μην είναι διαθέσιμα στο βασικό σύστημα. Στο τμήμα αυτό θα δούμε πως μπορείτε να τα εγκαταστήσετε.

Το τμήμα αυτό καλύπτει τις εφαρμογές:

Όνομα Εφαρμογής	Απαιτούμενοι Πόροι	Εγκατάσταση από Ports	Βασικές Εξαρτήσεις
Acrobat Reader®	λίγοι (ελαφριά)	ελαφριά	Δυαδική συμβατότητα με Linux (Linux Binary Compatibility)
gv	λίγοι (ελαφριά)	ελαφριά	Xaw3d
Xpdf	λίγοι (ελαφριά)	ελαφριά	FreeType
GQview	λίγοι (ελαφριά)	ελαφριά	Gtk+ ή GNOME

11.1. Acrobat Reader®

Πολλά έγγραφα διανέμονται πλέον ως αρχεία PDF το οποίο σημαίνει "Portable Document Format" (Φορητή Μορφή Εγγράφου). Ένα από τα συνιστώμενα προγράμματα προβολής για αυτό τον τύπο αρχείων είναι το Acrobat Reader®, το οποίο η Adobe διαθέτει για Linux. Καθώς το FreeBSD μπορεί να χρησιμοποιήσει εκτελέσιμα του Linux, η εφαρμογή είναι επίσης διαθέσιμη για το FreeBSD.

Για να εγκαταστήσετε το Acrobat Reader® 8 από τη Συλλογή των Ports, γράψτε:

```
# cd /usr/ports/print/acroread8
# make install clean
```

Δεν υπάρχει διαθέσιμο πακέτο, λόγω περιορισμών στην άδεια χρήσης.

11.2. gv

Το gv είναι ένα πρόγραμμα προβολής εγγράφων για αρχεία PostScript® και PDF. Είναι αρχικά βασισμένο στην εφαρμογή ghostview αλλά έχει καλύτερη εμφάνιση χάρη στη βιβλιοθήκη Xaw3d. Είναι γρήγορο, και το interface του είναι ξεκάθαρο. Το gv έχει πολλές δυνατότητες, όπως προσανατολισμό και μέγεθος χαρτιού, εμφάνιση υπό κλίμακα και βελτίωση εμφάνισης γραμματοσειρών (antialias). Σχεδόν κάθε λειτουργία του μπορεί να εκτελεστεί τόσο από το πληκτρολόγιο όσο και από το ποντίκι.

Για να εγκαταστήσετε το gv ως πακέτο, γράψτε:

```
# pkg_add -r gv
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports:

```
# cd /usr/ports/print/gv
# make install clean
```

11.3. Xpdf

Αν θέλετε ένα μικρό πρόγραμμα προβολής αρχείων PDF για το FreeBSD, το Xpdf είναι ελαφρύ και αποδοτικό. Απαιτεί ελάχιστους πόρους και είναι ιδιαίτερα σταθερό. Χρησιμοποιεί τις βασικές γραμματοσειρές των X και δεν απαιτεί χρήση του Motif® ή άλλης εργαλειοθήκης των X.

Για να εγκαταστήσετε το Xpdf ως πακέτο, δώστε την εντολή:

```
# pkg_add -r xpdf
```

Αν το πακέτο δεν είναι διαθέσιμο ή προτιμάτε να χρησιμοποιήσετε την Συλλογή των Ports, γράψτε:

```
# cd /usr/ports/graphics/xpdf
# make install clean
```

Μόλις ολοκληρωθεί η εγκατάσταση, μπορείτε να ξεκινήσετε το Xpdf και να χρησιμοποιήσετε το δεξί πλήκτρο του ποντικιού για να ενεργοποιήσετε το μενού.

11.4. GQview

Το GQview είναι ένας διαχειριστής εικόνων. Μπορείτε να δείτε ένα αρχείο με ένα απλό κλικ, να ξεκινήσετε ένα εξωτερικό πρόγραμμα επεξεργασίας, να δείτε προεπισκόπηση σε μορφή thumbnail και πολλά άλλα. Διαθέτει επίσης προβολή παρουσίασης και κάποιες βασικές λειτουργίες αρχείων. Μπορείτε να διαχειριστείτε συλλογές εικόνων και να βρείτε με εύκολο τρόπο τις διπλές. Το GQview μπορεί να χρησιμοποιηθεί για προβολή σε πλήρη οθόνη και υποστηρίζει τοπικές / διεθνείς ρυθμίσεις.

Αν θέλετε να εγκαταστήσετε το GQview ως πακέτο, γράψτε:

```
# pkg_add -r gqview
```

Αν το πακέτο δεν είναι διαθέσιμο, ή προτιμάτε να χρησιμοποιήσετε την Συλλογή των Ports, γράψτε:

```
# cd /usr/ports/graphics/gqview
# make install clean
```

Chapter 12. Χρηματοοικονομικές Εφαρμογές

Αν, για οποιοδήποτε λόγο, θέλετε να διαχειρίζεστε τα χρηματοοικονομικά σας μέσω του FreeBSD desktop σας, υπάρχουν κάποιες ισχυρές και εύκολες στη χρήση εφαρμογές, έτοιμες προς εγκατάσταση. Ορισμένες από αυτές είναι συμβατές με διαδεδομένες μορφές αρχείων, όπως αυτές που χρησιμοποιούνται στα έγγραφα του Quicken ή του Excel.

Το τμήμα αυτό καλύπτει τις εφαρμογές:

Όνομα Εφαρμογής	Απαιτούμενοι Πόροι	Εγκατάσταση Από Ports	Βασικές Εξαρτήσεις
GnuCash	λίγοι (ελαφριά)	βαριά	GNOME
Gnumeric	λίγοι (ελαφριά)	βαριά	GNOME
Abacus	λίγοι (ελαφριά)	ελαφριά	Tcl/Tk
KMyMoney	λίγοι (ελαφριά)	βαριά	KDE

12.1. GnuCash

Το GnuCash είναι μέρος της προσπάθειας του GNOME να παρέχει φιλικές εφαρμογές στους τελικούς χρήστες. Με το GnuCash, μπορείτε να κρατάτε λογαριασμό των εσόδων και εξόδων σας, των τραπεζικών σας λογαριασμών και των μετοχών σας. Διαθέτει περιβάλλον εργασίας το οποίο είναι εύκολο στη χρήση χωρίς να χρειάζεται ιδιαίτερη εκμάθηση, αλλά είναι ταυτόχρονα και πολύ επαγγελματικό.

Το GnuCash παρέχει έξυπνο σύστημα καταχώρησης, ιεραρχικό σύστημα λογαριασμών, πολλά πλήκτρα συντομεύσεων πληκτρολογίου, καθώς και μεθόδους αυτόματης συμπλήρωσης. Μπορεί να διαχωρίσει μια συναλλαγή σε πολλά λεπτομερή τμήματα. Το GnuCash μπορεί να εισάγει και να συγχωνεύσει αρχεία QIF του Quicken. Μπορεί επίσης να χειριστεί τις περισσότερες διεθνείς μορφές ημερομηνιών και νομισματικών μονάδων.

Για να εγκαταστήσετε το GnuCash στο σύστημα σας, γράψτε:

```
# pkg_add -r gnucash
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports:

```
# cd /usr/ports/finance/gnucash
# make install clean
```

12.2. Gnumeric

Το Gnumeric είναι ένα υπολογιστικό φύλλο και αποτελεί μέρος του περιβάλλοντος εργασίας GNOME. Διαθέτει βολική αυτόματη "πρόβλεψη" της εισόδου του χρήστη σύμφωνα με τη μορφή του κελιού καθώς και σύστημα αυτόματης συμπλήρωσης (autofill) για διάφορες ακολουθίες. Μπορεί να

εισάγει αρχεία διάφορων δημοφιλών μορφών, όπως αυτά που χρησιμοποιούνται στο Excel, το Lotus 1-2-3, ή το Quattro Pro. Το Gnumeric υποστηρίζει γραφήματα μέσω του προγράμματος γραφικών math/guppi. Έχει μεγάλο αριθμό ενσωματωμένων συναρτήσεων και επιτρέπει όλες τις συνήθεις μορφές κελιών, όπως αριθμούς, νομισματικές μονάδες, ημερομηνίες, ώρες και πολλές ακόμα.

Για να εγκαταστήσετε το Gnumeric ως πακέτο, γράψτε:

```
# pkg_add -r gnumeric
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports, γράφοντας:

```
# cd /usr/ports/math/gnumeric
# make install clean
```

12.3. Abacus

Το Abacus είναι ένα μικρό και εύκολο στη χρήση υπολογιστικό φύλλο. Περιλαμβάνει πολλές ενσωματωμένες συναρτήσεις οι οποίες είναι χρήσιμες σε διάφορα πεδία, όπως η στατιστική, τα χρηματοοικονομικά και τα μαθηματικά. Μπορεί να εισάγει και να εξάγει αρχεία του Excel. Το Abacus μπορεί να παράγει έξοδο μορφής PostScript®.

Για να εγκαταστήσετε το Abacus ως πακέτο, γράψτε:

```
# pkg_add -r abacus
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports, γράφοντας:

```
# cd /usr/ports/deskutils/abacus
# make install clean
```

12.4. KMyMoney

Το KMyMoney είναι μια εφαρμογή διαχείρισης των προσωπικών σας οικονομικών, φτιαγμένη για το περιβάλλον KDE. Το KMyMoney στοχεύει να παρέχει και να ενσωματώσει όλες τις λειτουργίες που διατίθενται σε αντίστοιχες εμπορικές εφαρμογές. Το KMyMoney μπορεί να εισάγει αρχεία του προτύπου QIF (Quicken Interchange Format), να τηρεί καταγραφή των επενδύσεων σας, να χειρίζεται πολλαπλές νομισματικές μονάδες και να παρέχει πλήθος αναφορών. Μέσα από ξεχωριστό plugin, παρέχεται επίσης η δυνατότητα εισαγωγής αρχείων OFX.

Για να εγκαταστήσετε το KMyMoney ως πακέτο, εκτελέστε την εντολή:

```
# pkg_add -r kmymoney2
```

Αν το πακέτο δεν είναι διαθέσιμο, μπορείτε να χρησιμοποιήσετε την Συλλογή των Ports, όπως φαίνεται παρακάτω:

```
# cd /usr/ports/finance/kmymoney2
# make install clean
```

Chapter 13. Περίληψη

Αν και το FreeBSD είναι δημοφιλές στους παροχείς Internet (ISPs) για την απόδοση και τη σταθερότητα του, είναι επίσης έτοιμο και για καθημερινή χρήση ως desktop. Με αρκετές χιλιάδες εφαρμογές διαθέσιμες ως πακέτα ή ports, μπορείτε να δημιουργήσετε το τέλειο desktop που καλύπτει όλες τις ανάγκες σας.

Παρακάτω, φαίνεται μια γρήγορη περίληψη όλων των desktop εφαρμογών που παρουσιάστηκαν σε αυτό το κεφάλαιο:

Όνομα Εφαρμογής	Όνομα Πακέτου	Όνομα Port
Opera	`opera`	www/opera
Firefox	`firefox`	www/firefox
Chromium	`chromium`	www/chromium
KOffice	`koffice-kde4`	editors/koffice-kde4
AbiWord	`abiword`	editors/abiword
The GIMP	`gimp`	graphics/gimp
OpenOffice.org	`openoffice`	editors/openoffice.org-3
LibreOffice	`libreoffice`	editors/libreoffice
Acrobat Reader®	`acroread`	print/acroread8
gv	`gv`	print/gv
Xpdf	`xpdf`	graphics/xpdf
GQview	`gqview`	graphics/gqview
GnuCash	`gnucash`	finance/gnucash
Gnumeric	`gnumeric`	math/gnumeric
Abacus	`abacus`	deskutils/abacus
KMyMoney	`kmymoney2`	finance/kmymoney2

Chapter 14. Πολυμέσα

14.1. Σύνοψη

Το FreeBSD υποστηρίζει μεγάλη ποικιλία από κάρτες ήχου, επιτρέποντας σας έτσι να απολαύσετε υψηλής πιστότητας ήχο από τον υπολογιστή σας. Περιλαμβάνεται η δυνατότητα να εγγράψετε και να αναπαράγετε ήχο MPEG Audio Layer 3 (MP3), WAV, και Ogg Vorbis καθώς και πολλά άλλα formats. Το FreeBSD Ports Collection επίσης περιέχει εφαρμογές που σας επιτρέπουν να επεξεργαστείτε τον ηχογραφημένο σας ήχο, να προσθέσετε ηχητικά εφέ, και να ελέγξετε συσκευές MIDI.

Με λίγο πειραματισμό, το FreeBSD μπορεί να υποστηρίξει αναπαραγωγή αρχείων video και DVD. Ο αριθμός των εφαρμογών που κωδικοποιούν, μετατρέπουν, και αναπαράγουν διάφορους τύπους video είναι πιο περιορισμένος από τον αριθμό των εφαρμογών ήχου. Για παράδειγμα, όταν γράφηκε αυτό το κείμενο, δεν υπήρχε καμιά καλή εφαρμογή επανακωδικοποίησης στη συλλογή των Ports του FreeBSD, που θα μπορούσε να χρησιμοποιηθεί για μετατροπή μεταξύ formats, όπως το audio/sox. Παρ' όλα αυτά, το τοπίο σε αυτό τον τομέα, και όσο αφορά το λογισμικό, αλλάζει ραγδαία.

Το κεφάλαιο αυτό θα περιγράψει τα απαραίτητα βήματα για τη ρύθμιση της κάρτας ήχου σας. Η ρύθμιση και εγκατάσταση του X11 (Το Σύστημα X Window) έχει ήδη φροντίσει για τα πιθανά προβλήματα υλικού της κάρτας γραφικών σας, αν και μπορεί να χρειάζεται να εφαρμόσετε κάποιες ακόμα μικρο-ρυθμίσεις για καλύτερη αναπαραγωγή.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να ρυθμίσετε το σύστημα σας ώστε να αναγνωρίζεται η κάρτα ήχου σας.
- Μεθόδους για να ελέγξετε τη λειτουργία της κάρτας σας.
- Πως να επιλύσετε προβλήματα σχετικά με τις ρυθμίσεις ήχου.
- Πως να αναπαράγετε και να κωδικοποιήσετε MP3 και άλλους τύπους αρχείων ήχου.
- Πως υποστηρίζεται το video από τον X server.
- Κάποια ports αναπαραγωγής/κωδικοποίησης video που δίνουν καλά αποτελέσματα.
- Πως να αναπαράγετε DVD, και αρχεία .mpg και .avi.
- Πως να κάνετε rip το περιεχόμενο CD και DVD σε αρχεία.
- Πως να ρυθμίσετε μια κάρτα τηλεόρασης.
- Πως να ρυθμίσετε ένα σαρωτή εικόνων.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ξέρετε πως θα ρυθμίσετε και θα εγκαταστήσετε νέο πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).

Αν προσπαθήσετε να προσαρτήσετε μουσικά CD με την εντολή mount(8) θα προκληθεί κατ' ελάχιστον σφάλμα, ή στη χειρότερη περίπτωση *kernel panic*. Τέτοια μέσα έχουν εξειδικευμένες κωδικοποιήσεις που διαφέρουν από το συνηθισμένο

σύστημα αρχείων ISO.

14.2. Ρύθμιση της Κάρτας Ήχου

14.2.1. Ρυθμίζοντας το Σύστημα

Πριν ξεκινήσετε, θα πρέπει να ξέρετε το μοντέλο της κάρτας που έχετε, το ολοκληρωμένο κύκλωμα που χρησιμοποιεί, καθώς και αν είναι PCI ή ISA. Το FreeBSD υποστηρίζει μεγάλη ποικιλία καρτών ήχου, τόσο PCI όσο και ISA. Ελέγξτε τις υποστηριζόμενες συσκευές ήχου στις Σημειώσεις Υλικού για να δείτε αν η κάρτα σας υποστηρίζεται. Στις Σημειώσεις Υλικού αναφέρεται επίσης ποιο πρόγραμμα οδήγησης υποστηρίζει την κάρτα σας.

Για να χρησιμοποιήσετε την συσκευή ήχου που διαθέτετε, θα πρέπει να φορτώσετε τον κατάλληλο οδηγό συσκευής. Αυτό μπορεί να επιτευχθεί με δύο τρόπους. Ο ευκολότερος είναι απλώς να φορτώσετε ένα module (άρθρωμα) για την κάρτα ήχου στον πυρήνα, χρησιμοποιώντας την εντολή kldload(8), με τη βοήθεια της γραμμής εντολών:

```
# kldload snd_emu10k1
```

ή προσθέτοντας την κατάλληλη γραμμή στο αρχείο /boot/loader.conf όπως παρακάτω:

```
snd_emu10k1_load="YES"
```

Τα παραπάνω παραδείγματα είναι για μια κάρτα ήχου Creative SoundBlaster® Live!. Υπάρχουν διαθέσιμα και άλλα modules για κάρτες ήχου και μπορείτε να τα δείτε στο αρχείο /boot/defaults/loader.conf. Αν δεν είστε σίγουρος για το πρόγραμμα οδήγησης που πρέπει να χρησιμοποιήσετε, μπορείτε να προσπαθήσετε να φορτώσετε το module snd_driver:

```
# kldload snd_driver
```

Πρόκειται για ένα μετα-πρόγραμμα οδήγησης, το οποίο φορτώνει με μιας όλα τα κοινά προγράμματα οδήγησης για κάρτες ήχου. Με τον τρόπο αυτό μπορείτε να επιταχύνετε την ανίχνευση για το σωστό οδηγό. Μπορείτε επίσης να φορτώσετε όλα τα προγράμματα οδήγησης μέσω του αρχείου /boot/loader.conf.

Αν επιθυμείτε να βρείτε το επιλεγμένο πρόγραμμα οδήγησης της κάρτας σας μετά τη φόρτωση του snd_driver, μπορείτε να ελέγξετε το αρχείο /dev/sndstat με την βοήθεια της εντολής `cat /dev/sndstat`.

Μια δεύτερη μέθοδος είναι να μεταγλωττίσετε την υποστήριξη της κάρτας ήχου σας, στατικά, απευθείας στον πυρήνα. Το παρακάτω τμήμα παρέχει τις πληροφορίες που χρειάζεστε για να προσθέσετε υποστήριξη για το υλικό σας με αυτό τον τρόπο. Για περισσότερες πληροφορίες σχετικά με την μεταγλώττιση του πυρήνα, δείτε το Ρυθμίζοντας τον Πυρήνα του FreeBSD.

14.2.1.1. Δημιουργώντας Προσαρμοσμένο Πυρήνα με Υποστήριξη Ήχου

Αρχικά, πρέπει να προσθέσετε το γενικό πρόγραμμα οδήγησης ήχου (audio framework driver) sound(4) στον πυρήνα σας. Θα χρειαστεί να προσθέσετε την ακόλουθη γραμμή στο αρχείο ρυθμίσεων του πυρήνα:

```
device sound
```

Έπειτα, θα πρέπει να προσθέσετε υποστήριξη για την κάρτα ήχου σας. Πρέπει να γνωρίζετε από πριν ποιο πρόγραμμα οδήγησης την υποστηρίζει. Ελέγξτε τη λίστα των υποστηριζόμενων καρτών στις Σημειώσεις Υλικού, για να καθορίσετε το σωστό οδηγό για την δική σας. Για παράδειγμα, ή Creative SoundBlaster® Live!, υποστηρίζεται από τον οδηγό snd_emu10k1(4). Για να προσθέσετε υποστήριξη για αυτή την κάρτα, χρησιμοποιήστε την ακόλουθη γραμμή:

```
device snd_emu10k1
```

Βεβαιωθείτε ότι διαβάσατε την σελίδα του manual για το πρόγραμμα οδήγησης, ώστε να χρησιμοποιήσετε τη σωστή σύνταξη. Η ακριβής σύνταξη για κάθε υποστηριζόμενη κάρτα ήχου στο αρχείο ρυθμίσεων πυρήνα, μπορεί να βρεθεί επίσης στο αρχείο /usr/src/sys/conf/NOTES.

Για κάρτα ήχου τύπου ISA που δεν είναι Plug'N'Play μπορεί να χρειαστεί να δώσετε στον πυρήνα πληροφορίες σχετικά με τις ρυθμίσεις της (όπως το IRQ, θύρα I/O κλπ), όπως γίνεται τυπικά σε αυτές τις περιπτώσεις. Αυτό μπορεί να γίνει μέσω του αρχείου /boot/device.hints. Κατά τη διαδικασία της εκκίνησης, ο loader(8) θα διαβάσει το αρχείο και θα μεταβιβάσει τις ρυθμίσεις στον πυρήνα. Για παράδειγμα, μια παλιά Creative SoundBlaster® 16 ISA μη-PnP κάρτα χρησιμοποιεί το πρόγραμμα οδήγησης snd_sbc(4) σε συνδυασμό με το `snd_sb16`. Για την κάρτα αυτή πρέπει να προστεθούν οι παρακάτω γραμμές στο αρχείο ρυθμίσεων πυρήνα:

```
device snd_sbc
device snd_sb16
```

και οι παρακάτω γραμμές στο αρχείο /boot/device.hints:

```
hint.sbc.0.at="isa"
hint.sbc.0.port="0x220"
hint.sbc.0.irq="5"
hint.sbc.0.drq="1"
hint.sbc.0.flags="0x15"
```

Στην περίπτωση αυτή, η κάρτα χρησιμοποιεί τη θύρα I/O `0x220` και το IRQ `5`.

Η σύνταξη που χρησιμοποιείται στο αρχείο /boot/device.hints εξηγείται στη σελίδα manual του sound(4) καθώς και στη σελίδα manual του αντίστοιχου προγράμματος οδήγησης.

Οι ρυθμίσεις που φαίνονται παραπάνω είναι οι προεπιλεγμένες. Σε ορισμένες περιπτώσεις, μπορεί να χρειαστεί να αλλάξετε το IRQ ή άλλες ρυθμίσεις ώστε να ταιριάζουν με τις ρυθμίσεις της κάρτας

σας. Δείτε τη σελίδα manual της snd_sbc(4) για περισσότερες πληροφορίες σχετικά με την κάρτα αυτή.

14.2.2. Δοκιμάζοντας την Κάρτα Ήχου

Αφού κάνετε επανεκκίνηση με τον νέο πυρήνα (ή αφού φορτώσετε το απαραίτητο module), Θα πρέπει να δείτε μηνύματα σχετικά με την κάρτα ήχου στην προσωρινή μνήμη (buffer) καταγραφής του συστήματος (dmesg(8)) αντίστοιχα με τα παρακάτω:

```
pcm0: <Intel ICH3 (82801CA)> port 0xdc80-0xdcbf,0xd800-0xd8ff irq 5 at device 31.5 on
pci0
pcm0: [GIANT-LOCKED]
pcm0: <Cirrus Logic CS4205 AC97 Codec>
```

Η κατάσταση της κάρτας ήχου μπορεί να ελεγχθεί μέσω του αρχείου /dev/sndstat:

```
# cat /dev/sndstat
FreeBSD Audio Driver (newpcm)
Installed devices:
pcm0: <Intel ICH3 (82801CA)> at io 0xd800, 0xdc80 irq 5 bufsz 16384
kld snd_ich (1p/2r/0v channels duplex default)
```

Τα μηνύματα στο σύστημα σας μπορεί να είναι διαφορετικά. Αν δεν δείτε συσκευές τύπου pcm, επιστρέψτε και ελέγξτε τα βήματα που κάνατε προηγουμένως. Κοιτάξτε το αρχείο ρυθμίσεων πυρήνα και βεβαιωθείτε ότι έχετε επιλέξει το σωστό πρόγραμμα οδήγησης. Για συνήθη προβλήματα και την αντιμετώπιση τους, δείτε το τμήμα Συνηθισμένα Προβλήματα.

Αν όλα πάνε καλά, η κάρτα ήχου σας θα λειτουργεί. Αν ο οδηγός CD ή DVD που διαθέτετε είναι συνδεμένος με την κάρτα ήχου μέσω της αναλογικής του εξόδου, μπορείτε να βάλετε ένα μουσικό CD και να το αναπαράγετε με το πρόγραμμα cdcontrol(1):

```
% cdcontrol -f /dev/acd0 play 1
```

Άλλες εφαρμογές, όπως το audio/workman παρέχουν φιλικότερο περιβάλλον εργασίας. Ίσως θέλετε να εγκαταστήσετε μια εφαρμογή όπως το audio/mpg123 για να αναπαράγετε αρχεία ήχου MP3.

Ένας άλλος γρήγορος τρόπος για να ελέγξετε την κάρτα ήχου σας, είναι να στείλετε δεδομένα στην συσκευή /dev/dsp, όπως παρακάτω:

```
% cat filename > /dev/dsp
```

όπου το filename μπορεί να είναι οποιοδήποτε αρχείο. Η παραπάνω εντολή θα πρέπει να παράγει κάποιο ήχο (θόρυβο) επιβεβαιώνοντας τη σωστή λειτουργία της κάρτας ήχου.

Τα αρχεία συσκευών /dev/dsp* δημιουργούνται αυτόματα όταν χρειάζεται. Δεν

> υπάρχουν αν δεν χρησιμοποιούνται και δεν θα εμφανιστούν στην έξοδο της ls(1)

Η ένταση ήχου της κάρτας μπορεί να αλλάξει μέσω της εντολής mixer(8). Περισσότερες πληροφορίες μπορείτε να βρείτε στην σελίδα του manual της mixer(8).

14.2.2.1. Συνηθισμένα Προβλήματα

Πρόβλημα	Λύση
`sb_dspwr(XX) timed out`	Δεν είναι σωστά ρυθμισμένη η θύρα I/O.
`bad irq XX`	Το IRQ δεν είναι σωστά ρυθμισμένο. Βεβαιωθείτε ότι το IRQ που έχετε δηλώσει είναι το ίδιο με αυτό που έχει ρυθμιστεί στην κάρτα.
`xxx: gus pcm not attached, out of memory`	Δεν υπάρχει αρκετή διαθέσιμη μνήμη για να γίνει χρήση της συσκευής.
`xxx: can't open /dev/dsp!`	Ελέγξτε με την βοήθεια της εντολής `fstat | grep dsp` αν κάποια άλλη εφαρμογή απασχολεί τη συγκεκριμένη συσκευή. Συνήθεις ύποπτοι είναι η εφαρμογή esound καθώς και το σύστημα υποστήριξης ήχου του περιβάλλοντος KDE.

Ένα ακόμα πρόβλημα δημιουργείται από ορισμένες σύγχρονες κάρτες γραφικών οι οποίες περιέχουν μια δική τους συσκευή ήχου για χρήση μέσω συνδέσεων HDMI ή αντίστοιχων. Σε ορισμένες περιπτώσεις, είναι πιθανόν αυτή η συσκευή να εντοπισθεί πριν την κανονική κάρτα ήχου με αποτέλεσμα να πάρει τη θέση της προεπιλεγμένης συσκευής ήχου. Για να ελέγξετε αν συμβαίνει αυτό, εκτελέστε την εντολή dmesg και ψάξτε για τη λέξη `pcm`. Η έξοδος θα μοιάζει με την παρακάτω:

```
...
hdac0: HDA Driver Revision: 20100226_0142
hdac1: HDA Driver Revision: 20100226_0142
hdac0: HDA Codec #0: NVidia (Unknown)
hdac0: HDA Codec #1: NVidia (Unknown)
hdac0: HDA Codec #2: NVidia (Unknown)
hdac0: HDA Codec #3: NVidia (Unknown)
pcm0: <HDA NVidia (Unknown) PCM #0 DisplayPort> at cad 0 nid 1 on hdac0
pcm1: <HDA NVidia (Unknown) PCM #0 DisplayPort> at cad 1 nid 1 on hdac0
pcm2: <HDA NVidia (Unknown) PCM #0 DisplayPort> at cad 2 nid 1 on hdac0
pcm3: <HDA NVidia (Unknown) PCM #0 DisplayPort> at cad 3 nid 1 on hdac0
hdac1: HDA Codec #2: Realtek ALC889
pcm4: <HDA Realtek ALC889 PCM #0 Analog> at cad 2 nid 1 on hdac1
pcm5: <HDA Realtek ALC889 PCM #1 Analog> at cad 2 nid 1 on hdac1
pcm6: <HDA Realtek ALC889 PCM #2 Digital> at cad 2 nid 1 on hdac1
pcm7: <HDA Realtek ALC889 PCM #3 Digital> at cad 2 nid 1 on hdac1
...
```

Στο παράδειγμα μας, η κάρτα γραφικών (`NVidia`) εντοπίστηκε πριν την κανονική κάρτα ήχου (`Realtek ALC889`). Για να χρησιμοποιήσετε την πραγματική κάρτα ήχου ως την προεπιλεγμένη

συσκευή ήχου, αλλάξτε το hw.snd.default_unit όπως φαίνεται παρακάτω:

```
# sysctl hw.snd.default_unit=n
```

Το *n* είναι ο αριθμός της συσκευής που θα χρησιμοποιηθεί, στο παράδειγμα μας το 4. Προσθέστε την παρακάτω γραμμή στο /etc/sysctl.conf για να γίνει μόνιμη αυτή η αλλαγή:

```
hw.snd.default_unit=4
```

14.2.3. Χρησιμοποιώντας Πολλαπλές Πηγές Ήχου

Είναι πολλές φορές επιθυμητό να έχουμε πολλαπλές πηγές ήχου που να αναπαράγονται ταυτόχρονα, όπως όταν για παράδειγμα το esound ή το artsd δεν επιτρέπουν κοινή χρήση της συσκευής ήχου σε κάποια συγκεκριμένη εφαρμογή.

Το FreeBSD επιτρέπει αυτή τη λειτουργία μέσω των *Εικονικών Καναλιών Ήχου (Virtual Sound Channels)*, τα οποία μπορούν να ενεργοποιηθούν μέσω των δυνατοτήτων που παρέχονται από το sysctl(8). Τα Εικονικά Κανάλια σας επιτρέπουν να πολυπλέξετε τους ήχους που αναπαράγει η κάρτα σας, αναμιγνύοντας τον ήχο στον πυρήνα.

Για να ρυθμίσετε το πλήθος των εικονικών καναλιών, υπάρχουν τρεις ρυθμίσεις sysctl που μπορούν να γίνουν αν είστε ο χρήστης root, όπως φαίνεται παρακάτω:

```
# sysctl dev.pcm.0.play.vchans=4
# sysctl dev.pcm.0.rec.vchans=4
# sysctl hw.snd.maxautovchans=4
```

Το παραπάνω παράδειγμα παραχωρεί τέσσερα εικονικά κανάλια, τα οποία άνετα επαρκούν για καθημερινή χρήση. Οι τιμές dev.pcm.0.play.vchans=4 και dev.pcm.0.rec.vchans=4 αναφέρονται στον αριθμό των εικονικών καναλιών που διαθέτει η συσκευή pcm0 για αναπαραγωγή και εγγραφή, και μπορούν να ρυθμιστούν μετά την προσάρτηση της συσκευής. Η μεταβλητή hw.snd.maxautovchans είναι ο αριθμός των εικονικών καναλιών που παραχωρούνται σε μια νέα συσκευή ήχου όταν αυτή προσαρτάται μέσω της εντολής kldload(8). Καθώς το module pcm μπορεί να φορτωθεί ανεξάρτητα από τα προγράμματα οδήγησης του υλικού, το hw.snd.maxautovchans μπορεί να αποθηκεύσει το μέγιστο πλήθος των εικονικών καναλιών που θα παραχωρηθούν σε όσες συσκευές ήχου προσαρτηθούν αργότερα. Δείτε τη σελίδα manual pcm(4) για περισσότερες λεπτομέρειες.

Δεν μπορείτε να αλλάξετε τον αριθμό των εικονικών καναλιών μιας συσκευής όσο αυτή είναι σε χρήση. Πρώτα κλείστε όσα προγράμματα χρησιμοποιούν τη συσκευή, όπως προγράμματα αναπαραγωγής μουσικής ή δαίμονες ήχου.

Η σωστή συσκευή pcm αποδίδεται αυτόματα και διάφανα σε κάθε πρόγραμμα που ζητά να χρησιμοποιήσει το /dev/dsp0.

14.2.4. Ρυθμίζοντας Προεπιλεγμένες Τιμές για τα Κανάλια του Μίκτη

Οι προεπιλεγμένες τιμές για τα διάφορα κανάλια του μίκτη, είναι ενσωματωμένες στον πηγαίο κώδικα του προγράμματος οδήγησης pcm(4). Υπάρχουν πολλές διαφορετικές εφαρμογές και δαίμονες που σας επιτρέπουν να αλλάξετε τιμές στο μίκτη, απομνημονεύοντας τις μεταξύ διαδοχικών κλήσεων, αλλά ή λύση αυτή δεν είναι και η καλύτερη. Είναι δυνατόν να ορίσετε προεπιλεγμένες τιμές μίξης σε επίπεδο προγράμματος οδήγησης. Αυτό μπορεί να επιτευχθεί με την ρύθμιση κατάλληλων τιμών στο αρχείο /boot/device.hints, π.χ.:

```
hint.pcm.0.vol="50"
```

Το παραπάνω ρυθμίζει την ένταση του ήχου στην προεπιλεγμένη τιμή 50, όταν φορτωθεί το module pcm(4).

14.3. Ήχος MP3

Τα αρχεία ήχου MP3 (MPEG Layer 3 Audio) επιτυγχάνουν ποιότητα ήχου πολύ κοντά στο μουσικό CD, και είναι καλό να έχετε δυνατότητα αναπαραγωγής τους στο FreeBSD σύστημα σας.

14.3.1. Προγράμματα Αναπαραγωγής MP3

Το πιο δημοφιλές, με μεγάλη διαφορά, πρόγραμμα αναπαραγωγής MP3 για το X11, είναι η εφαρμογή XMMS (X Multimedia System). Μπορείτε να χρησιμοποιήσετε τα skins του Winamp με το XMMS καθώς το γραφικό του περιβάλλον είναι σχεδόν όμοιο με το Winamp της Nullsoft. Το XMMS έχει επίσης ενσωματωμένη δυνατότητα χρήσης plug-ins.

Το XMMS μπορεί να εγκατασταθεί από το port multimedia/xmms ή από πακέτο.

Το περιβάλλον του XMMS το καθιστά εύκολο στη χρήση, καθώς διαθέτει λίστα αναπαραγωγής (playlist), γραφικό ισοσταθμιστή και άλλες λειτουργίες. Όσοι είναι εξοικειωμένοι με το Winamp θα βρουν το XMMS απλό στη χρήση του.

Το port audio/mpg123 είναι ένα εναλλακτικό πρόγραμμα αναπαραγωγής MP3 μέσω της γραμμής εντολών.

Το mpg123 μπορεί να εκτελεστεί καθορίζοντας τη συσκευή ήχου και το αρχείο MP3 στη γραμμή εντολών. Θεωρώντας ότι η συσκευή ήχου είναι το /dev/dsp1.0 και θέλετε να αναπαράγετε το αρχείο *Foobar-GreatestHits.mp3*, θα χρησιμοποιήσετε την παρακάτω εντολή:

```
# mpg123 -a /dev/dsp1.0 Foobar-GreatestHits.mp3
High Performance MPEG 1.0/2.0/2.5 Audio Player for Layer 1, 2 and 3.
Version 0.59r (1999/Jun/15). Written and copyrights by Michael Hipp.
Uses code from various people. See 'README' for more!
THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTY! USE AT YOUR OWN RISK!

Playing MPEG stream from Foobar-GreatestHits.mp3 ...
MPEG 1.0 layer III, 128 kbit/s, 44100 Hz joint-stereo
```

14.3.2. Αποθήκευση (Rip) Αρχείων από Μουσικά CD

Πριν κωδικοποιήσετε ένα ολόκληρο CD ή ένα κομμάτι από CD σε αρχείο MP3, θα πρέπει να αντιγράψετε τα μουσικά δεδομένα από το CD στο σκληρό σας δίσκο. Αυτό γίνεται γράφοντας τα δεδομένα τύπου CDDA (CD Digital Audio) σε αρχεία WAV.

Το εργαλείο `cdda2wav`, το οποίο ανήκει στη συλλογή εργαλείων sysutils/cdrtools μπορεί να χρησιμοποιηθεί τόσο για την ανάκτηση των δεδομένων ήχου από μουσικά CD, όσο και πληροφοριών που σχετίζονται με αυτά.

Έχοντας το μουσικό CD στον οδηγό, μπορείτε να χρησιμοποιήσετε την ακόλουθη εντολή (ως `root`) για να αποθηκεύσετε ένα ολόκληρο CD σε χωριστά (ανά κομμάτι) αρχεία WAV:

```
# cdda2wav -D 0,1,0 -B
```

Το cdda2wav υποστηρίζει οδηγούς CDROM τύπου ATAPI (IDE). Για να διαβάσετε δεδομένα από μια συσκευή IDE, χρησιμοποιήστε το όνομα συσκευής αντί για τον αριθμό μονάδας SCSI. Για παράδειγμα, για να αποθηκεύσετε το κομμάτι 7 από ένα οδηγό IDE:

```
# cdda2wav -D /dev/acd0 -t 7
```

Το `-D 0,1,0` δείχνει τη συσκευή SCSI 0,1,0, που αντιστοιχεί στην έξοδο της εντολής `cdrecord -scanbus`.

Για να διαβάσετε μεμονωμένα κομμάτια, χρησιμοποιήστε την επιλογή `-t` όπως φαίνεται παρακάτω:

```
# cdda2wav -D 0,1,0 -t 7
```

Το παράδειγμα αυτό διαβάζει το κομμάτι επτά του μουσικού CD. Για να διαβάσετε μια σειρά από κομμάτια, για παράδειγμα από το ένα ως το επτά, καθορίστε μια περιοχή:

```
# cdda2wav -D 0,1,0 -t 1+7
```

Μπορείτε επίσης να χρησιμοποιήσετε το βοηθητικό πρόγραμμα dd(1) για να διαβάσετε μουσικά κομμάτια από οδηγούς ATAPI. Διαβάστε το Duplicating Audio CDs για περισσότερες πληροφορίες σχετικά με αυτή τη δυνατότητα.

14.3.3. Κωδικοποιώντας MP3

Στις μέρες μας, το προτιμώμενο πρόγραμμα κωδικοποίησης είναι το Lame. Μπορείτε να το βρείτε στη συλλογή των ports, στο audio/lame.

Χρησιμοποιώντας τα αρχεία WAV που έχετε αποθηκεύσει, μπορείτε να μετατρέψετε το αρχείο audio01.wav σε audio01.mp3 με την εντολή:

```
# lame -h -b 128 \
--tt "Foo Song Title" \
--ta "FooBar Artist" \
--tl "FooBar Album" \
--ty "2001" \
--tc "Ripped and encoded by Foo" \
--tg "Genre" \
audio01.wav audio01.mp3
```

Τα 128 kbits είναι η τυπικά χρησιμοποιούμενη ποιότητα για αρχεία MP3. Ωστόσο, πολλοί προτιμούν μεγαλύτερη ποιότητα όπως 160 ή 192. Όσο μεγαλύτερος είναι ο ρυθμός δεδομένων (bitrate), τόσο περισσότερο χώρο αποθήκευσης θα χρειάζεται το αρχείο MP3 που θα προκύψει, ωστόσο και η ποιότητα θα είναι υψηλότερη. Η επιλογή `-h` ενεργοποιεί τη δυνατότητα "υψηλότερης ποιότητας αλλά ελαφρά πιο αργής κωδικοποίησης". Οι επιλογές που ξεκινούν με `--t` δείχνουν ετικέτες (tags) ID3, οι οποίες συνήθως περιέχουν πληροφορίες σχετικές με το τραγούδι και οι οποίες μπορούν να ενσωματωθούν μέσα σε αρχεία MP3. Μπορείτε να βρείτε περισσότερες επιλογές σχετικά με την κωδικοποίηση, αν συμβουλευτείτε τη σελίδα manual του προγράμματος lame.

14.3.4. Αποκωδικοποιώντας MP3

Για να μπορέσετε να γράψετε μουσικό CD από αρχεία MP3, θα πρέπει να τα μετατρέψετε ξανά σε μορφή ασυμπίεστου αρχείου WAV. Τόσο το XMMS όσο και το mpg123 υποστηρίζουν εξαγωγή αρχείου MP3 σε ασυμπίεστη μορφή αρχείου.

Γράφοντας στο Δίσκο μέσω του XMMS:

1. Ξεκινήστε το XMMS.
2. Κάντε δεξί κλικ στο παράθυρο της εφαρμογής για να ανοίξετε το μενού του XMMS.
3. Επιλέξτε `Preferences` από τα `Options`.
4. Αλλάξτε το Output Plugin σε "Disk Writer Plugin".
5. Πιέστε `Configure`.
6. Γράψτε (ή επιλέξτε browse) ένα κατάλογο για να αποθηκεύσετε τα αποσυμπιεσμένα αρχεία.
7. Φορτώστε το αρχείο MP3 στο XMMS όπως συνήθως, με την ένταση στο 100% και τις ρυθμίσεις EQ ανενεργές.
8. Πιέστε το `Play`. Το XMMS θα φαίνεται ότι αναπαράγει το MP3, αλλά δεν θα ακούγεται κανείς ήχος. Στην πραγματικότητα αναπαράγει το MP3 σε αρχείο.
9. Όταν τελειώσετε, βεβαιωθείτε ότι επαναφέρατε τη ρύθμιση του προεπιλεγμένου Output Plugin στην προηγούμενη επιλογή της, για να μπορέσετε να ακούσετε ξανά αρχεία MP3.

Γράφοντας στην έξοδο μέσω του mpg123:

1. Εκτελέστε `mpg123 -s audio01.mp3 > audio01.pcm`

Το XMMS γράφει αρχεία σε μορφή WAV, ενώ το mpg123 μετατρέπει το MP3 σε μη- επεξεργασμένα (raw) δεδομένα ήχου PCM. Και οι δύο αυτές μορφές μπορούν να χρησιμοποιηθούν με την εφαρμογή

cdrecord για τη δημιουργία μουσικών CD. Για την εφαρμογή burncd(8) θα πρέπει να χρησιμοποιήσετε δεδομένα PCM. Αν χρησιμοποιήσετε αρχεία WAV θα παρατηρήσετε ένα μικρό ήχο (tick) στην αρχή κάθε κομματιού. Ο ήχος αυτός προέρχεται από την επικεφαλίδα (header) του αρχείου WAV. Μπορείτε να αφαιρέσετε την επικεφαλίδα με τη βοήθεια του προγράμματος SoX (μπορείτε να το εγκαταστήσετε από το port audio/sox ή το αντίστοιχο πακέτο):

```
% sox -t wav -r 44100 -s -w -c 2 track.wav track.raw
```

Διαβάστε το Creating and Using CD Media για περισσότερες πληροφορίες σχετικά με τη χρήση CD εγγραφής στο FreeBSD

14.4. Αναπαραγωγή Video

Η αναπαραγωγή video είναι μια καινούρια και ραγδαία αναπτυσσόμενη περιοχή εφαρμογών. Θα χρειαστεί να δείξετε υπομονή. Δεν πρόκειται να λειτουργήσουν όλα τόσο ομαλά όπως στον ήχο.

Πριν ξεκινήσετε, θα πρέπει να γνωρίζετε το μοντέλο της κάρτας γραφικών που έχετε καθώς και το ολοκληρωμένο κύκλωμα που χρησιμοποιεί. Αν και το Xorg υποστηρίζει μεγάλη γκάμα από κάρτες γραφικών, αυτές που παρέχουν καλή απόδοση είναι λιγότερες. Για να πάρετε μια λίστα των εκτεταμένων δυνατοτήτων που υποστηρίζονται από την κάρτα σας, χρησιμοποιήστε την εντολή xdpyinfo(1) την ώρα που εκτελούνται τα X11.

Είναι γενικά καλή ιδέα να έχετε ένα μικρό αρχείο MPEG το οποίο μπορεί να χρησιμοποιηθεί για δοκιμές διαφορετικών επιλογών και προγραμμάτων αναπαραγωγής. Κάποια προγράμματα αναπαραγωγής DVD αναζητούν από προεπιλογή το δίσκο DVD στη συσκευή /dev/dvd. Σε ορισμένα το όνομα της συσκευής είναι ενσωματωμένο στον κώδικα του προγράμματος. Για το λόγο αυτό, ίσως είναι χρήσιμο να φτιάξετε συμβολικές συνδέσεις προς τις πραγματικές συσκευές:

```
# ln -sf /dev/acd0 /dev/dvd
# ln -sf /dev/acd0 /dev/rdvd
```

Σημειώστε ότι λόγω της φύσης του συστήματος devfs(5), αυτού του είδους οι συνδέσεις δεν παραμένουν μετά την επανεκκίνηση του συστήματος σας. Για να δημιουργούνται οι συμβολικές συνδέσεις αυτόματα σε κάθε εκκίνηση του συστήματος σας, προσθέστε τις ακόλουθες γραμμές στο αρχείο /etc/devfs.conf:

```
link acd0 dvd
link acd0 rdvd
```

Επιπρόσθετα, η αποκωδικοποίηση DVD, η οποία χρειάζεται κλήση ειδικών λειτουργιών του DVD-ROM, απαιτεί και άδεια εγγραφής (write permission) στις συσκευές DVD.

Για τη βελτίωση της λειτουργίας της κοινόχρηστης μνήμης του συστήματος X11, συνίσταται να αυξήσετε τις τιμές κάποιων μεταβλητών sysctl(8):

```
kern.ipc.shmmax=67108864
kern.ipc.shmall=32768
```

14.4.1. Προσδιορισμός Δυνατοτήτων Κάρτας Γραφικών

Υπάρχουν αρκετοί διαφορετικοί τρόποι για την απεικόνιση video στο X11. Το τι θα δουλέψει τελικά, εξαρτάται σε μεγάλο βαθμό από το υλικό σας. Κάθε μέθοδος που περιγράφουμε παρακάτω θα δώσει διαφορετική ποιότητα σε διαφορετικό υλικό. Επίσης, η αναπαραγωγή video στο X11 είναι ένα θέμα στο οποίο πρόσφατα δίνεται μεγάλη σημασία, και πιθανόν θα υπάρχουν αρκετές βελτιώσεις σε κάθε νέα έκδοση του Xorg.

Κατάλογος κοινών διεπαφών video:

1. X11: Συνηθισμένη έξοδος του X11 με χρήση κοινόχρηστης μνήμης.
2. XVideo: μια επέκταση της διεπαφής X11 που υποστηρίζει αναπαραγωγή video σε οποιαδήποτε σχεδιάσιμη επιφάνεια του X11.
3. SDL: Simple Directmedia Layer.
4. DGA: Direct Graphics Access.
5. SVGAlib: Επίπεδο γραφικών χαμηλού επιπέδου για κονσόλα.

14.4.1.1. XVideo

Το Xorg διαθέτει μια επέκταση που ονομάζεται *XVideo* (γνωστή και ως Xvideo, Xv, xv) και το οποίο επιτρέπει την απευθείας απεικόνιση video σε σχεδιάσιμα αντικείμενα μέσω ειδικής επιτάχυνσης. Η επέκταση αυτή παρέχει αναπαραγωγή πολύ καλής ποιότητας, ακόμα και σε μηχανήματα χαμηλών προδιαγραφών.

Για να δείτε αν χρησιμοποιείται η επέκταση, χρησιμοποιήστε την εντολή `xvinfo`:

```
% xvinfo
```

Το XVideo υποστηρίζεται από την κάρτα σας αν το αποτέλεσμα δείχνει όπως παρακάτω:

```
X-Video Extension version 2.2
screen #0
  Adaptor #0: "Savage Streams Engine"
    number of ports: 1
    port base: 43
    operations supported: PutImage
    supported visuals:
      depth 16, visualID 0x22
      depth 16, visualID 0x23
    number of attributes: 5
      "XV_COLORKEY" (range 0 to 16777215)
              client settable attribute
              client gettable attribute (current value is 2110)
```

```
      "XV_BRIGHTNESS" (range -128 to 127)
              client settable attribute
              client gettable attribute (current value is 0)
      "XV_CONTRAST" (range 0 to 255)
              client settable attribute
              client gettable attribute (current value is 128)
      "XV_SATURATION" (range 0 to 255)
              client settable attribute
              client gettable attribute (current value is 128)
      "XV_HUE" (range -180 to 180)
              client settable attribute
              client gettable attribute (current value is 0)
    maximum XvImage size: 1024 x 1024
    Number of image formats: 7
      id: 0x32595559 (YUY2)
        guid: 59555932-0000-0010-8000-00aa00389b71
        bits per pixel: 16
        number of planes: 1
        type: YUV (packed)
      id: 0x32315659 (YV12)
        guid: 59563132-0000-0010-8000-00aa00389b71
        bits per pixel: 12
        number of planes: 3
        type: YUV (planar)
      id: 0x30323449 (I420)
        guid: 49343230-0000-0010-8000-00aa00389b71
        bits per pixel: 12
        number of planes: 3
        type: YUV (planar)
      id: 0x36315652 (RV16)
        guid: 52563135-0000-0000-0000-000000000000
        bits per pixel: 16
        number of planes: 1
        type: RGB (packed)
        depth: 0
        red, green, blue masks: 0x1f, 0x3e0, 0x7c00
      id: 0x35315652 (RV15)
        guid: 52563136-0000-0000-0000-000000000000
        bits per pixel: 16
        number of planes: 1
        type: RGB (packed)
        depth: 0
        red, green, blue masks: 0x1f, 0x7e0, 0xf800
      id: 0x31313259 (Y211)
        guid: 59323131-0000-0010-8000-00aa00389b71
        bits per pixel: 6
        number of planes: 3
        type: YUV (packed)
      id: 0x0
        guid: 00000000-0000-0000-0000-000000000000
        bits per pixel: 0
```

```
        number of planes: 0
        type: RGB (packed)
        depth: 1
        red, green, blue masks: 0x0, 0x0, 0x0
```

Παρατηρήστε επίσης ότι τα formats που εμφανίζονται (YUV2, YUV12, κ.λ.π.) δεν διατίθενται σε όλες τις εκδόσεις του XVideo, και η απουσία τους μπορεί να επηρεάσει κάποια προγράμματα αναπαραγωγής.

Αν το αποτέλεσμα δείχνει κάπως έτσι:

```
X-Video Extension version 2.2
screen #0
no adaptors present
```

Τότε πιθανώς το XVideo δεν υποστηρίζεται από την κάρτα σας.

Αν το XVideo δεν υποστηρίζεται από την κάρτα σας, αυτό σημαίνει απλά ότι θα είναι πιο δύσκολο ο υπολογιστής σας να ανταποκριθεί στις υπολογιστικές απαιτήσεις της απεικόνισης video. Ωστόσο, ανάλογα με την κάρτα γραφικών και τον επεξεργαστή σας, είναι ακόμα πιθανόν να έχετε ικανοποιητική αναπαραγωγή. Ίσως πρέπει να διαβάσετε μεθόδους για τη βελτίωση της απόδοσης, στα προχωρημένα θέματα, Επιπλέον Διάβασμα.

14.4.1.2. Το Επίπεδο Simple Directmedia Layer

Το Simple Directmedia Layer, SDL, προορίζονταν να γίνει ένα επίπεδο συμβατότητας μεταξύ των Microsoft® Windows®, BeOS, και του UNIX®, επιτρέποντας ανάπτυξη εφαρμογών ήχου και εικόνας, κατάλληλες για κάθε μια από αυτές τις πλατφόρμες (cross-platform). Το επίπεδο SDL παρέχει χαμηλού επιπέδου πρόσβαση στο υλικό, και σε ορισμένες περιπτώσεις μπορεί να είναι πιο αποδοτικό από την διεπαφή X11.

Το SDL μπορεί να βρεθεί στο devel/sdl12.

14.4.1.3. Το Επίπεδο Direct Graphics Access

Το Direct Graphics Access είναι μια επέκταση του X11 που επιτρέπει σε ένα πρόγραμμα να προσπεράσει τον X server και να αλλάξει απευθείας τα περιεχόμενα του framebuffer (μνήμης γραφικών). Δεδομένου ότι βασίζεται σε διαχείριση μνήμης χαμηλού επιπέδου, τα προγράμματα που το χρησιμοποιούν πρέπει να εκτελούνται ως `root`.

Η επέκταση DGA μπορεί να ελεγχθεί και να μετρηθεί ως προς την απόδοση της με το πρόγραμμα dga(1). Όταν εκτελείται η εντολή `dga`, αλλάζει τα χρώματα της οθόνης σε κάθε πίεση ενός πλήκτρου. Για να ακυρώσετε την εκτέλεση, πιέστε `q`.

14.4.2. Πακέτα και Ports που Σχετίζονται με Video

Το τμήμα αυτό περιγράφει το λογισμικό που διατίθεται στη συλλογή των ports του FreeBSD και το οποίο μπορεί να χρησιμοποιηθεί για αναπαραγωγή video. Ο τομέας της αναπαραγωγής video είναι

ιδιαίτερα ενεργός όσο αφορά την ανάπτυξη λογισμικού, και έτσι οι δυνατότητες των εφαρμογών πιθανώς να αποκλίνουν κάπως από αυτές που περιγράφονται εδώ.

Είναι αρχικά σημαντικό να γνωρίζετε ότι αρκετές από τις εφαρμογές video που εκτελούνται στο FreeBSD αναπτύχθηκαν αρχικά ως εφαρμογές Linux. Πολλές από αυτές τις εφαρμογές είναι ακόμα ποιότητας beta. Κάποια από τα προβλήματα που μπορεί να συναντήσετε στις εφαρμογές video του FreeBSD περιλαμβάνουν:

1. Μια εφαρμογή δεν μπορεί να αναπαράγει ένα αρχείο που δημιουργήθηκε από κάποια άλλη.
2. Μια εφαρμογή δεν μπορεί να αναπαράγει ένα αρχείο που δημιούργησε η ίδια.
3. Η ίδια εφαρμογή, σε δυο διαφορετικά μηχανήματα, και αφού έχει μεταγλωττιστεί σε κάθε μηχάνημα ειδικά για αυτό, αναπαράγει το ίδιο αρχείο με διαφορετικό τρόπο.
4. Κάποιο φαινομενικά απλό φίλτρο, όπως αυτό της αλλαγής μεγέθους εικόνας (rescaling), έχει ως αποτέλεσμα την δημιουργία κακής ποιότητας video (τεχνουργημάτων) εξαιτίας προβληματικής ρουτίνας μεγέθυνσης
5. Κάποια εφαρμογή τερματίζεται απότομα συχνά.
6. Δεν εγκαθίσταται η τεκμηρίωση του προγράμματος κατά την εγκατάσταση του port, ενώ μπορεί να βρεθεί είτε στο δικτυακό τόπο του προγράμματος είτε στον κατάλογο work του port.

Πολλές από τις εφαρμογές αυτές μπορεί επίσης να παρουσιάσουν συμπτώματα "Linux-ισμού". Μπορεί δηλ. να εμφανίζουν προβλήματα που οφείλονται στον τρόπο με τον οποίο υλοποιούνται κάποιες στάνταρ βιβλιοθήκες στις διανομές του Linux, ή ίσως οι συγγραφείς να έχουν θεωρήσει ως δεδομένες κάποιες δυνατότητες του πυρήνα όπως υπάρχουν στο Linux. Τα προβλήματα αυτά δεν είναι σίγουρο ότι ανακαλύπτονται και διορθώνονται πάντα από τους συντηρητές του port, το οποίο μπορεί να οδηγήσει σε προβλήματα όπως τα παρακάτω:

1. Χρήση του αρχείου /proc/cpuinfo για την ανίχνευση των δυνατοτήτων του επεξεργαστή.
2. Κακή χρήση των threads (νημάτων) το οποίο οδηγεί το πρόγραμμα σε κόλλημα αντί για κανονικό τερματισμό στο τέλος της εκτέλεσης.
3. Χρήση λογισμικού που δεν υπάρχει ακόμα στη συλλογή των ports του FreeBSD σε συνδυασμό με την εφαρμογή.

Μέχρι στιγμής οι συγγραφείς των εφαρμογών αυτών έχουν αποδειχθεί συνεργάσιμοι με τους συντηρητές των ports, ώστε να ελαχιστοποιηθούν οι επεμβάσεις που χρειάζονται για την μετατροπή (porting) των εφαρμογών.

14.4.2.1. MPlayer

Ο MPlayer είναι μια εφαρμογή αναπαραγωγής video που αναπτύχθηκε πρόσφατα και εξελίσσεται ταχύτατα. Οι στόχοι της ομάδας ανάπτυξης του MPlayer είναι η ταχύτητα και η ευελιξία στο Linux και στα άλλα Unix. Η δημιουργία του ξεκίνησε όταν ο αρχηγός της ομάδας ανάπτυξης κουράστηκε να αντιμετωπίζει τα προβλήματα αναπαραγωγής των μέχρι τότε διαθέσιμων προγραμμάτων. Κάποιοι υποστηρίζουν ότι το γραφικό περιβάλλον θυσιάστηκε για να δημιουργηθεί μια ομοιόμορφη σχεδίαση. Ωστόσο, μόλις συνηθίσετε τις επιλογές που δίνονται από τη γραμμή εντολών και τα αντίστοιχα πλήκτρα, θα μπορέσετε να τον χρησιμοποιήσετε αρκετά καλά.

14.4.2.1.1. Μεταγλώττιση του MPlayer

Ο MPlayer βρίσκεται στο multimedia/mplayer. Ο MPlayer κάνει πλήθος ελέγχων του υλικού κατά τη διαδικασία της μεταγλώττισης, φτιάχνοντας έτσι ένα εκτελέσιμο το οποίο δεν έχει φορητότητα από ένα σύστημα σε ένα άλλο. Για το σκοπό αυτό, είναι σημαντικό να τον εγκαταστήσετε από τα ports και όχι από έτοιμο πακέτο. Επιπρόσθετα, μπορείτε να καθορίσετε πλήθος επιλογών στην γραμμή εντολών του `make` όπως περιγράφεται στο Makefile και κατά την έναρξη της διαδικασίας μεταγλώττισης:

```
# cd /usr/ports/multimedia/mplayer
# make
N - O - T - E

Take a careful look into the Makefile in order
to learn how to tune mplayer towards you personal preferences!
For example,
make WITH_GTK1
builds MPlayer with GTK1-GUI support.
If you want to use the GUI, you can either install
/usr/ports/multimedia/mplayer-skins
or download official skin collections from
http://www.mplayerhq.hu/homepage/dload.html
```

Οι προεπιλεγμένες επιλογές μάλλον είναι κατάλληλες για τους περισσότερους χρήστες. Αν ωστόσο χρειάζεστε τον αποκωδικοποιητή XviD, θα πρέπει να καθορίσετε την επιλογή `WITH_XVID` στην γραμμή εντολών. Μπορείτε επίσης να ορίσετε την προεπιλεγμένη συσκευή DVD χρησιμοποιώντας την επιλογή `WITH_DVD_DEVICE`, διαφορετικά θα χρησιμοποιηθεί η προεπιλεγμένη συσκευή /dev/acd0.

Όταν γράφονταν αυτό το κείμενο, το port του MPlayer δημιουργούσε επίσης την τεκμηρίωση του προγράμματος και δύο εκτελέσιμα, τον `mplayer`, και τον `mencoder`, το οποίο είναι ένα εργαλείο για επανακωδικοποίηση video.

Η HTML τεκμηρίωση του MPlayer είναι ιδιαίτερα πληροφοριακή. Αν ο αναγνώστης βρει ότι οι πληροφορίες αυτού του κεφαλαίου όσο αφορά το υλικό και τις διεπαφές video είναι ελλιπείς, η τεκμηρίωση του MPlayer αποτελεί ένα ιδιαίτερα αναλυτικό συμπλήρωμα. Θα πρέπει σίγουρα να διαθέσετε χρόνο για να διαβάσετε την τεκμηρίωση του MPlayer αν αναζητάτε πληροφορίες σχετικά με την υποστήριξη video στο UNIX®.

14.4.2.1.2. Χρησιμοποιώντας τον MPlayer

Κάθε χρήστης του MPlayer πρέπει να δημιουργήσει ένα υποκατάλογο .mplayer μέσα στον προσωπικό του κατάλογο. Για να δημιουργήσετε τον απαραίτητο υποκατάλογο, μπορείτε να γράψετε το παρακάτω:

```
% cd /usr/ports/multimedia/mplayer
% make install-user
```

Οι επιλογές της γραμμής εντολών του `mplayer` περιγράφονται στη σελίδα του manual. Για ακόμα

περισσότερες λεπτομέρειες, υπάρχει τεκμηρίωση σε μορφή HTML. Στο τμήμα αυτό θα περιγράψουμε μερικές μόνο κοινές χρήσεις.

Για να αναπαράγετε ένα αρχείο, όπως το testfile.avi, μέσω ενός από τα αρκετά video interfaces χρησιμοποιήστε την επιλογή `-vo`:

```
% mplayer -vo xv testfile.avi
```

```
% mplayer -vo sdl testfile.avi
```

```
% mplayer -vo x11 testfile.avi
```

```
# mplayer -vo dga testfile.avi
```

```
# mplayer -vo 'sdl:dga' testfile.avi
```

Αξίζει τον κόπο να δοκιμάσετε όλες αυτές τις επιλογές, καθώς η απόδοση τους εξαρτάται από πολλούς παράγοντες και διαφοροποιείται αρκετά ανάλογα με το υλικό του υπολογιστή σας.

Για αναπαραγωγή από DVD, αντικαταστήστε το testfile.avi με `dvd://N -dvd-device DEVICE` όπου το *N* είναι ο αριθμός του τίτλου (title number) που επιθυμείτε να αναπαράγετε και DEVICE είναι το όνομα συσκευής του DVD-ROM. Για παράδειγμα, για να αναπαράγετε τον τίτλο 3 από τη συσκευή /dev/dvd:

```
# mplayer -vo xv dvd://3 -dvd-device /dev/dvd
```

Η προεπιλεγμένη συσκευή DVD μπορεί να καθοριστεί κατά τη διάρκεια της μεταγλώττισης του MPlayer port μέσω της επιλογής `WITH_DVD_DEVICE`. Από προεπιλογή, η συσκευή αυτή είναι η /dev/acd0. Μπορείτε να βρείτε περισσότερες πληροφορίες στο αρχείο Makefile του port.

Για τα πλήκτρα που χρησιμοποιούνται για παύση, διακοπή, μετακίνηση κλπ. κατά τη διάρκεια της αναπαραγωγής, συμβουλευτείτε την βοήθεια που μπορείτε να δείτε εκτελώντας `mplayer -h` ή διαβάστε τη σελίδα του manual.

Επιπρόσθετα, σημαντικές επιλογές αναπαραγωγής είναι: `-fs -zoom` το οποίο ενεργοποιεί απεικόνιση σε πλήρη οθόνη και το `-framedrop` το οποίο βοηθάει στην αύξηση της απόδοσης.

Για να μείνει το μέγεθος της γραμμής εντολών το δυνατόν μικρό, ο χρήστης μπορεί να δημιουργήσει ένα αρχείο .mplayer/config και να ορίσει εκεί τις προεπιλεγμένες επιλογές:

```
vo=xv
```

```
fs=yes
zoom=yes
```

Τέλος, ο mplayer μπορεί να χρησιμοποιηθεί για την εξαγωγή (rip) ενός τίτλου DVD σε ένα αρχείο .vob file. Για την εξαγωγή του δεύτερου τίτλου από ένα DVD, γράψτε:

```
# mplayer -dumpstream -dumpfile out.vob dvd://2 -dvd-device /dev/dvd
```

Το αρχείο εξόδου, out.vob, θα είναι τύπου MPEG και μπορείτε να το μεταχειριστείτε μέσω άλλων πακέτων video που περιγράφονται σε αυτό το τμήμα.

14.4.2.1.3. mencoder

Πριν χρησιμοποιήσετε το mencoder είναι καλή ιδέα να εξοικειωθείτε με τις επιλογές που αναφέρονται στην τεκμηρίωση HTML. Υπάρχει σελίδα manual, αλλά δεν είναι πολύ χρήσιμη χωρίς την HTML τεκμηρίωση. Υπάρχουν πάρα πολλοί τρόποι για να βελτιώσετε την ποιότητα, να μειώσετε το ρυθμό δεδομένων (bitrate) να αλλάξετε μορφή αρχείου, και κάποια από αυτά τα κόλπα μπορεί να κάνουν τη διαφορά μεταξύ καλής και κακής απόδοσης. Εδώ θα δείτε μερικά παραδείγματα για να ξεκινήσετε. Πρώτα μια απλή αντιγραφή:

```
% mencoder input.avi -oac copy -ovc copy -o output.avi
```

Λανθασμένοι συνδυασμοί στη γραμμή εντολών, μπορεί να δώσουν αρχεία εξόδου τα οποία δεν μπορεί να αναπαράγει ούτε ο ίδιος ο mplayer. Έτσι, αν απλώς θέλετε να κάνετε rip ένα αρχείο, μείνετε στην επιλογή -dumpfile του mplayer.

Για να μετατρέψετε το input.avi σε codec MPEG4 με ήχο MPEG3 (απαιτείται το audio/lame):

```
% mencoder input.avi -oac mp3lame -lameopts br=192 \
     -ovc lavc -lavcopts vcodec=mpeg4:vhq -o output.avi
```

Με τον τρόπο αυτό παράγεται έξοδος που μπορεί να αναπαραχθεί από τον mplayer και το xine.

Μπορείτε να αντικαταστήσετε το input.avi με την επιλογή dvd://1 -dvd-device /dev/dvd και να το εκτελέσετε ως root για να επανακωδικοποιήσετε απευθείας ένα τίτλο DVD. Μια και πιθανώς δεν θα μείνετε ικανοποιημένος με το αποτέλεσμα από την πρώτη φορά, σας συνιστούμε να κατεβάσετε τον τίτλο σε ένα αρχείο και να δουλέψετε σε αυτό.

14.4.2.2. Το Πρόγραμμα Αναπαραγωγής xine

Το xine είναι ένα project με ευρύ σκοπό, το οποίο προορίζεται όχι μόνο να γίνει ένα πρόγραμμα όλα σε ένα όσο αφορά το video, αλλά επίσης στο να παράγει μια επαναχρησιμοποιήσιμη βασική βιβλιοθήκη και ένα αρθρωτό εκτελέσιμο το οποίο μπορεί να επεκταθεί με πρόσθετα (plugins). Μπορείτε να το εγκαταστήσετε τόσο από πακέτο, όσο και από το port, multimedia/xine.

Το xine είναι ακόμα κάπως χοντροκομμένο, αλλά σίγουρα έχει ξεκινήσει καλά. Στην πράξη, το xine

χρειάζεται είτε γρήγορο επεξεργαστή και κάρτα γραφικών, ή υποστήριξη της επέκτασης XVideo. Το γραφικό περιβάλλον είναι χρησιμοποιήσιμο, αλλά κάπως αδέξια φτιαγμένο.

Την ώρα που γράφονταν αυτές οι γραμμές δεν διανέμονταν module μαζί με την εφαρμογή xine, ικανό να αναπαράγει DVD με CSS κωδικοποίηση. Υπάρχουν εκδόσεις από τρίτους κατασκευαστές οι οποίες έχουν ενσωματωμένο το παραπάνω module αλλά καμιά από αυτές δεν βρίσκεται στην συλλογή των ports του FreeBSD.

Σε σύγκριση με τον MPlayer, το xine κάνει περισσότερα για το χρήστη, αλλά την ίδια στιγμή, δεν επιτρέπει τόσο λεπτομερειακό έλεγχο. Το xine αποδίδει καλύτερα σε λειτουργία XVideo.

Από προεπιλογή, το xine θα ξεκινήσει σε γραφικό περιβάλλον (GUI). Μπορείτε να χρησιμοποιήσετε το μενού για να ανοίξετε ένα συγκεκριμένο αρχείο:

```
% xine
```

Εναλλακτικά, μπορείτε να το καλέσετε να αναπαράγει ένα αρχείο απευθείας από την γραμμή εντολών, χωρίς τη χρήση του GUI:

```
% xine -g -p mymovie.avi
```

14.4.2.3. Τα Βοηθητικά Προγράμματα transcode

Η εφαρμογή transcode δεν είναι πρόγραμμα αναπαραγωγής, αλλά μια σουίτα εργαλείων για επανακωδικοποίηση αρχείων video και ήχου. Με την εφαρμογή transcode, έχετε την δυνατότητα να αναμίξετε αρχεία video, να επισκευάσετε χαλασμένα αρχεία, χρησιμοποιώντας εργαλεία της γραμμής εντολών τα οποία χειρίζονται δεδομένα από τα κανάλια stdin/stdout.

Μεγάλο πλήθος εφαρμογών μπορούν να καθοριστούν κατά τη διάρκεια της μεταγλώττισης του port multimedia/transcode και συνιστούμε την ακόλουθη γραμμή εντολών για τη μεταγλώττιση του transcode:

```
# make WITH_OPTIMIZED_CFLAGS=yes WITH_LIBA52=yes WITH_LAME=yes WITH_OGG=yes \
WITH_MJPEG=yes -DWITH_XVID=yes
```

Οι προτεινόμενες επιλογές είναι κατάλληλες για τους περισσότερους χρήστες.

Για να σας δείξουμε τις ικανότητες του `transcode`, δείτε ένα παράδειγμα μετατροπής αρχείου DivX σε PAL MPEG-1 (PAL VCD):

```
% transcode -i input.avi -V --export_prof vcd-pal -o output_vcd
% mplex -f 1 -o output_vcd.mpg output_vcd.m1v output_vcd.mpa
```

Το αρχείο MPEG που προκύπτει, το output_vcd.mpg, μπορεί να αναπαραχθεί από τον MPlayer. Μπορείτε επίσης να γράψετε το αρχείο σε ένα CD-R για να δημιουργήσετε ένα Video CD, και στην περίπτωση αυτή θα χρειαστεί να εγκαταστήσετε τα προγράμματα multimedia/vcdimager και

sysutils/cdrdao.

Υπάρχει σελίδα manual για το `transcode`, αλλά πρέπει επίσης να συμβουλευτείτε το transcode wiki για περισσότερες πληροφορίες και παραδείγματα.

14.4.3. Επιπλέον Διάβασμα

Υπάρχει ραγδαία εξέλιξη στα διαθέσιμα πακέτα video για το FreeBSD. Είναι αρκετά πιθανό ότι στο άμεσο μέλλον πολλά από τα προβλήματα που αναφέρονται εδώ θα έχουν επιλυθεί. Στο ενδιάμεσο διάστημα, όσοι ενδιαφέρονται να χρησιμοποιήσουν τις δυνατότητες A/V του FreeBSD στο έπακρο θα πρέπει να συνδυάσουν γνώσεις από διάφορα FAQ και tutorials και να χρησιμοποιήσουν αρκετές διαφορετικές εφαρμογές. Το τμήμα αυτό υπάρχει ακριβώς για να δείξει στον αναγνώστη που μπορεί να βρει τέτοιες πρόσθετες πληροφορίες.

Η Τεκμηρίωση του Mplayer είναι αρκετά πληροφοριακή όσο αφορά το τεχνικό επίπεδο. Αν έχετε σκοπό να αποκτήσετε υψηλό ποσοστό εμπειρίας σε σχέση με το video στο UNIX®, θα πρέπει οπωσδήποτε να την συμβουλευτείτε. Η λίστα αλληλογραφίας του MPlayer είναι εχθρική σε όποιον δεν έχει κάνει τον κόπο να διαβάσει την τεκμηρίωση, έτσι αν σκοπεύετε να κάνετε αναφορές σφαλμάτων, βεβαιωθείτε ότι την έχετε διαβάσει.

Το xine HOWTO περιέχει ένα κεφάλαιο σχετικά με την βελτίωση της απόδοσης, το οποίο είναι κοινό για όλα τα προγράμματα αναπαραγωγής.

Τέλος, υπάρχουν κάποιες άλλες πολλά υποσχόμενες εφαρμογές που ίσως επιθυμείτε να δοκιμάσετε:

- Το Avifile το οποίο είναι επίσης port, multimedia/avifile.
- Το Ogle το οποίο είναι επίσης port, multimedia/ogle.
- Το Xtheater
- Το multimedia/dvdauthor, το οποίο είναι εφαρμογή DVD authoring ανοικτού κώδικα.

14.5. Ρύθμιση Κάρτας Τηλεόρασης

14.5.1. Εισαγωγή

Οι κάρτες τηλεόρασης σας επιτρέπουν να βλέπετε τηλεόραση, κανονική ή καλωδιακή, στον υπολογιστή σας. Οι περισσότερες από αυτές δέχονται επίσης σήμα σύνθετου (composite) video, μέσω εισόδου RCA ή S-video, και κάποιες από αυτές διαθέτουν και ραδιοφωνικό δέκτη FM.

Το FreeBSD παρέχει υποστήριξη για κάρτες TV τύπου PCI που χρησιμοποιούν τα ολοκληρωμένα κυκλώματα σύλληψης video, Brooktree Bt848/849/878/879 ή Conexant CN-878/Fusion 878a με το πρόγραμμα οδήγησης bktr(4). Θα πρέπει επίσης να βεβαιωθείτε ότι η κάρτα έρχεται με δέκτη που υποστηρίζεται. Συμβουλευτείτε τη σελίδα manual του bktr(4) για να δείτε τη λίστα των υποστηριζόμενων δεκτών.

14.5.2. Εγκαθιστώντας το Πρόγραμμα Οδήγησης

Για να χρησιμοποιήσετε την κάρτα θα πρέπει να φορτώσετε το πρόγραμμα οδήγησης bktr(4), προσθέτοντας την ακόλουθη γραμμή στο αρχείο /boot/loader.conf:

```
bktr_load="YES"
```

Εναλλακτικά, μπορείτε να προσθέσετε στατική υποστήριξη για την κάρτα στο πυρήνα σας, και για το σκοπό αυτό προσθέστε τις ακόλουθες γραμμές στο αρχείο ρυθμίσεων του πυρήνα:

```
device  bktr
device  iicbus
device  iicbb
device  smbus
```

Οι επιπρόσθετοι οδηγοί συσκευών είναι απαραίτητοι, επειδή τα εξαρτήματα της κάρτας επικοινωνούν μεταξύ τους διαμέσου ενός διαύλου I2C. Αφού κάνετε τις απαραίτητες αλλαγές στο αρχείο, μεταγλωττίστε και εγκαταστήστε το νέο πυρήνα.

Μόλις τελειώσετε με αυτή τη διαδικασία, θα πρέπει να επανεκκινήσετε το σύστημα σας. Κατά τη διάρκεια της εκκίνησης, θα πρέπει να δείτε κάποια μηνύματα από την κάρτα σας, όπως τα παρακάτω:

```
bktr0: <BrookTree 848A> mem 0xd7000000-0xd7000fff irq 10 at device 10.0 on pci0
iicbb0: <I2C bit-banging driver> on bti2c0
iicbus0: <Philips I2C bus> on iicbb0 master-only
iicbus1: <Philips I2C bus> on iicbb0 master-only
smbus0: <System Management Bus> on bti2c0
bktr0: Pinnacle/Miro TV, Philips SECAM tuner.
```

Φυσικά, τα μηνύματα αυτά θα διαφέρουν ανάλογα με το υλικό σας. Ωστόσο θα πρέπει να ελέγξετε ότι ανιχνεύθηκε σωστά ο δέκτης. Είναι δυνατόν να αλλάξετε κάποιες από τις παραμέτρους που ανιχνεύθηκαν χρησιμοποιώντας MIBs του sysctl(8) καθώς και επιλογές στο αρχείο ρυθμίσεων πυρήνα. Για παράδειγμα, να θέλετε να επιβάλετε ο δέκτης να είναι τύπου Philips SECAM, θα πρέπει να προσθέσετε την ακόλουθη γραμμή στο αρχείο ρυθμίσεων του πυρήνα σας:

```
options OVERRIDE_TUNER=6
```

ή μπορείτε να χρησιμοποιήσετε απευθείας το sysctl(8):

```
# sysctl hw.bt848.tuner=6
```

Δείτε τη σελίδα manual του bktr(4) καθώς και το αρχείο /usr/src/sys/conf/NOTES για περισσότερες λεπτομέρειες σχετικά με τις διαθέσιμες επιλογές.

14.5.3. Χρήσιμες Εφαρμογές

Για να χρησιμοποιήσετε την κάρτα τηλεόρασης, θα πρέπει να εγκαταστήσετε μια από τις παρακάτω εφαρμογές:

- Το multimedia/fxtv παρέχει δυνατότητα να δείτε τηλεόραση σε παράθυρο, καθώς και την δυνατότητα σύλληψης εικόνας / ήχου / video.
- Το multimedia/xawtv είναι επίσης εφαρμογή τηλεόρασης, με δυνατότητες όμοιες με το fxtv.
- Το misc/alevt αποκωδικοποιεί και απεικονίζει Videotext/Teletext.
- Το audio/xmradio είναι μια εφαρμογή για να χρησιμοποιήσετε το δέκτη FM που είναι ενσωματωμένος σε κάποιες κάρτες τηλεόρασης.
- Το audio/wmtune είναι μια βολική desktop εφαρμογή για ραδιοφωνικούς δέκτες.

Μπορείτε να βρείτε περισσότερες εφαρμογές στη συλλογή των Ports του FreeBSD.

14.5.4. Αντιμετώπιση Προβλημάτων

Αν αντιμετωπίσετε κάποιο πρόβλημα με την κάρτα τηλεόρασης, θα πρέπει πρώτα να ελέγξετε αν το ολοκληρωμένο σύλληψης video καθώς και ο δέκτης υποστηρίζονται από το πρόγραμμα οδήγησης bktr(4) και αν έχετε χρησιμοποιήσει τις σωστές ρυθμίσεις στις επιλογές σας. Για επιπλέον υποστήριξη καθώς και διάφορες ερωτήσεις σχετικά με την κάρτα σας, ίσως θέλετε να επικοινωνήσετε με τη λίστα ηλεκτρονική λίστα του FreeBSD για τα πολυμέσα και να διαβάσετε τις παλιότερες δημοσιεύσεις από τα αρχεία της λίστας.

14.6. MythTV

Το MythTV είναι ένα πρόγραμμα τύπου PVR (Προσωπικός καταγραφέας video).

Στον κόσμο του Linux® το MythTV είναι ένα γνωστό πρόγραμμα με πολλές εξαρτήσεις οι οποίες δυσκολεύουν την εγκατάσταση του. Το port του FreeBSD απλοποιεί το μεγαλύτερο μέρος της διαδικασίας αλλά ορισμένα τμήματα του πρέπει να εγκατασταθούν χειροκίνητα. Η ενότητα αυτή περιέχει οδηγίες που θα σας βοηθήσουν να ρυθμίσετε το MythTV.

14.6.1. Υλικό

Το MythTV έχει σχεδιαστεί να χρησιμοποιεί το V4L για την πρόσβαση σε συσκευές video όπως κωδικοποιητές (encoders) και δέκτες. Τη δεδομένη στιγμή, το MythTV λειτουργεί καλύτερα με κάρτες DVB-S/C/T με διασύνδεση USB που υποστηρίζονται από το multimedia/webcamd καθώς το webcamd παρέχει μια εφαρμογή χρήστη για το V4L. Οποιαδήποτε κάρτα DVB που υποστηρίζεται από το webcamd θα πρέπει φυσιολογικά να λειτουργεί με το MythTV. Μπορείτε ωστόσο να βρείτε εδώ μια λίστα με δοκιμάσμενες κάρτες. Για κάρτες τις Hauppauge μπορείτε να βρείτε προγράμματα οδήγησης στα πακέτα multimedia/pvr250 και multimedia/pvrxxx, αλλά να έχετε υπόψη σας ότι χρησιμοποιούν μια μη-τυποποιημένη διεπαφή η οποία δεν λειτουργεί με εκδόσεις του MythTV μεταγενέστερες της 0.23.

Το HTPC περιέχει μια λίστα όλων των διαθέσιμων προγραμμάτων οδήγησης DVB.

14.6.2. Εξαρτήσεις

Καθώς το MythTV είναι ευέλικτο και αρθρωτό, επιτρέπει στο χρήστη να έχει το frontend και το backend σε διαφορετικά μηχανήματα.

Για το frontend, απαιτείται το multimedia/mythtv-frontend και ο εξυπηρετητής X τον οποίο μπορείτε να βρείτε στο x11/xorg. Ιδανικά, ο υπολογιστής που θα εκτελεί το frontend θα πρέπει επίσης να έχει μια κάρτα γραφικών η οποία να υποστηρίζει XvMC και προαιρετικά ένα τηλεχειριστήριο συμβατό με LIRC.

Για το backend, χρειάζεται το multimedia/mythtv όπως και μια βάση δεδομένων MySQL™ και προαιρετικά ένας δέκτης και αποθηκευτικός χώρος για εγγραφές. Το πακέτο για την MySQL™ θα πρέπει να εγκατασταθεί αυτόματα ως εξάρτηση κατά την εγκατάσταση του multimedia/mythtv.

14.6.3. Εγκατάσταση MythTV

Για να εγκαταστήσετε το MythTV, χρησιμοποιήστε τα παρακάτω βήματα. Αρχικά εγκαταστήστε το MythTV από την Συλλογή των Ports του FreeBSD:

```
# cd /usr/ports/multimedia/mythtv
# make install
```

Εγκαταστήστε τη βάση δεδομένων του MythTV:

```
# mysql -uroot -p < /usr/local/shared/mythtv/database/mc.sql
```

Ρυθμίστε το backend:

```
# mythtv-setup
```

Ξεκινήστε το backend:

```
# echo 'mythbackend_enable="YES"' >> /etc/rc.conf
# /usr/local/etc/rc.d/mythbackend start
```

14.7. Σαρωτές Εικόνας

14.7.1. Εισαγωγή

Στο FreeBSD η πρόσβαση σε σαρωτές παρέχεται από το SANE (Scanner Access Now Easy) API το οποίο διατίθεται μέσα από την συλλογή των Ports του FreeBSD. Το SANE χρησιμοποιεί επίσης κάποιους οδηγούς συσκευών του FreeBSD για να αποκτήσει πρόσβαση στο υλικό του σαρωτή.

Το FreeBSD υποστηρίζει σαρωτές SCSI και USB. Βεβαιωθείτε ότι ο σαρωτής σας υποστηρίζεται από το SANE πριν ξεκινήσετε οποιαδήποτε εγκατάσταση και ρύθμιση. Το SANE διαθέτει μια λίστα υποστηριζόμενων συσκευών η οποία παρέχει πληροφορίες για την υποστήριξη κάθε σαρωτή και την εξέλιξη της. Σε συστήματα πριν το FreeBSD 8.X θα βρείτε επίσης τη λίστα των υποστηριζόμενων USB σαρωτών στη σελίδα manual του uscanner(4).

14.7.2. Ρύθμιση του Πυρήνα

Όπως είπαμε παραπάνω, υποστηρίζονται σαρωτές τόσο SCSI όσο και USB. Ανάλογα με το τρόπο διασύνδεσης του σαρωτή σας, θα χρειαστείτε διαφορετικούς οδηγούς συσκευών.

14.7.2.1. Διασύνδεση USB

Ο πυρήνας GENERIC, από προεπιλογή, περιέχει τους οδηγούς συσκευών που απαιτούνται για την υποστήριξη σαρωτών USB. Αν αποφασίσετε να χρησιμοποιήσετε εξειδικευμένο πυρήνα, βεβαιωθείτε ότι έχετε τις ακόλουθες γραμμές στο αρχείο ρυθμίσεων σας:

```
device usb
device uhci
device ohci
device ehci
```

Σε συστήματα πριν το FreeBSD 8.X, θα χρειαστείτε επίσης την παρακάτω γραμμή:

```
device uscanner
```

Σε αυτές τις εκδόσεις του FreeBSD, η υποστήριξη των σαρωτών USB γίνεται μέσω της συσκευής uscanner(4). Από το FreeBSD 8.0 και μετά, η υποστήριξη αυτή παρέχεται απευθείας από τη βιβλιοθήκη libusb(3).

Αφού επανεκκινήσετε με το σωστό πυρήνα, συνδέστε το USB σαρωτή σας. Θα πρέπει να δείτε μια γραμμή σχετική με την ανίχνευση του σαρωτή στην προσωρινή μνήμη μηνυμάτων του συστήματος (dmesg(8)):

```
ugen0.2: <EPSON> at usbus0
```

ή σε ένα σύστημα FreeBSD 7.X:

```
uscanner0: EPSON EPSON Scanner, rev 1.10/3.02, addr 2
```

Τα μηνύματα αυτά δείχνουν ότι ο σαρωτής μας χρησιμοποιεί την συσκευή /dev/ugen0.2 ή την συσκευή /dev/uscanner0 ανάλογα με την έκδοση του FreeBSD που χρησιμοποιείται. Στο παράδειγμα μας, χρησιμοποιήσαμε ένα σαρωτή EPSON Perfection® 1650 USB.

14.7.2.2. Διασύνδεση Τύπου SCSI

Αν ο σαρωτής σας έρχεται με διασύνδεση τύπου SCSI, είναι σημαντικό να γνωρίζετε τι κάρτα ελεγκτή SCSI θα χρησιμοποιήσετε. Ανάλογα με το ολοκληρωμένο κύκλωμα της κάρτας SCSI που χρησιμοποιείται, θα πρέπει να ρυθμίσετε κατάλληλα το αρχείο ρυθμίσεων πυρήνα. Ο πυρήνας GENERIC υποστηρίζει τους πιο κοινούς ελεγκτές SCSI. Βεβαιωθείτε ότι διαβάσατε το αρχείο NOTES και προσθέστε τη σωστή γραμμή στο αρχείο ρυθμίσεων πυρήνα. Εκτός από το πρόγραμμα οδήγησης

του ελεγκτή SCSI, θα πρέπει ακόμα να έχετε τις ακόλουθες γραμμές στο αρχείο ρυθμίσεων του πυρήνα σας:

```
device scbus
device pass
```

Μόλις μεταγλωττίσετε και εγκαταστήσετε τον πυρήνα, θα μπορέσετε να δείτε τις συσκευές στην προσωρινή μνήμη μηνυμάτων συστήματος, κατά τη διάρκεια της εκκίνησης:

```
pass2 at aic0 bus 0 target 2 lun 0
pass2: <AGFA SNAPSCAN 600 1.10> Fixed Scanner SCSI-2 device
pass2: 3.300MB/s transfers
```

Αν ο σαρωτής σας δεν ήταν ενεργοποιημένος κατά την εκκίνηση του συστήματος σας, είναι ακόμα δυνατόν να εξαναγκάσετε τον εντοπισμό του, εκτελώντας ανίχνευση του διαύλου SCSI με την βοήθεια της εντολής camcontrol(8):

```
# camcontrol rescan all
Re-scan of bus 0 was successful
Re-scan of bus 1 was successful
Re-scan of bus 2 was successful
Re-scan of bus 3 was successful
```

Ο σαρωτής θα εμφανιστεί τότε στη λίστα των συσκευών SCSI:

```
# camcontrol devlist
<IBM DDRS-34560 S97B>              at scbus0 target 5 lun 0 (pass0,da0)
<IBM DDRS-34560 S97B>              at scbus0 target 6 lun 0 (pass1,da1)
<AGFA SNAPSCAN 600 1.10>           at scbus1 target 2 lun 0 (pass3)
<PHILIPS CDD3610 CD-R/RW 1.00>     at scbus2 target 0 lun 0 (pass2,cd0)
```

Περισσότερες πληροφορίες σχετικά με τις συσκευές SCSI είναι διαθέσιμες στις σελίδες manual scsi(4) και camcontrol(8).

14.7.3. Ρύθμιση του SANE

Το σύστημα SANE χωρίζεται σε δύο κομμάτια: στο backend (graphics/sane-backends) και στο frontend (graphics/sane-frontends). Το backend παρέχει πρόσβαση στον ίδιο το σαρωτή. Στη λίστα υποστηριζόμενων συσκευών του SANE μπορείτε να βρείτε ποιο backend υποστηρίζει τον σαρωτή σας. Είναι υποχρεωτικό να βρείτε το σωστό backend για να μπορέσετε να χρησιμοποιήσετε το σαρωτή σας. Το τμήμα του frontend παρέχει το γραφικό περιβάλλον εργασίας για τη σάρωση (xscanimage).

Το πρώτο βήμα είναι να εγκαταστήσετε το port ή το πακέτο graphics/sane-backends. Μετά χρησιμοποιήστε την εντολή `sane-find-scanner` για να ελέγξετε την ανίχνευση του σαρωτή σας από

το σύστημα SANE:

```
# sane-find-scanner -q
found SCSI scanner "AGFA SNAPSCAN 600 1.10" at /dev/pass3
```

Η έξοδος θα σας δείξει το είδος σύνδεσης του σαρωτή καθώς και το όνομα συσκευής που χρησιμοποιείται για τη σύνδεση με το σύστημα σας. Το όνομα του κατασκευαστή και του μοντέλου ίσως να μην εμφανιστούν, αλλά αυτό δεν είναι σημαντικό.

Ορισμένοι USB σαρωτές απαιτούν τη φόρτωση firmware. Η διαδικασία εξηγείται στη σελίδα manual του backend. Θα πρέπει επίσης να διαβάσετε τις σελίδες manual sane-find-scanner(1) και linprocfs(7).

Πρέπει τώρα να ελέγξουμε αν ο σαρωτής θα αναγνωριστεί από το frontend πρόγραμμα σάρωσης. Από προεπιλογή, το SANE backend έρχεται με ένα εργαλείο γραμμής εντολών, το sane(1). Η εντολή αυτή σας επιτρέπει την απαρίθμηση των συσκευών και τη σάρωσης εικόνας από τη γραμμή εντολών. Η επιλογή `-L` χρησιμοποιείται για την απαρίθμηση των συσκευών σάρωσης:

```
# scanimage -L
device `snapscan:/dev/pass3' is a AGFA SNAPSCAN 600 flatbed scanner
```

Ή για παράδειγμα με τον σαρωτή που χρησιμοποιήσαμε στο Διασύνδεση USB:

```
# scanimage -L
device 'epson2:libusb:/dev/usb:/dev/ugen0.2' is a Epson GT-8200 flatbed scanner
```

Η παραπάνω έξοδος προέρχεται από ένα σύστημα FreeBSD 8.X και η γραμμή `'epson2:libusb:/dev/usb:/dev/ugen0.2'` μας πληροφορεί για το όνομα του backend (`epson2`) και το όνομα της συσκευής (`/dev/ugen0.2`) που χρησιμοποιεί ο σαρωτής μας.

Αν δεν δείτε έξοδο, ή δείτε ένα μήνυμα ότι δεν ανιχνεύθηκε σαρωτής, σημαίνει ότι το sane(1) δεν μπόρεσε να αναγνωρίσει το σαρωτή. Αν συμβεί αυτό, θα χρειαστεί να επεξεργαστείτε το αρχείο ρυθμίσεων του backend και να ορίσετε το σαρωτή που θα χρησιμοποιηθεί. Ο κατάλογος /usr/local/etc/sane.d/ περιέχει όλα τα αρχεία ρυθμίσεων του backend. Το πρόβλημα αναγνώρισης εμφανίζεται σε ορισμένα μοντέλα USB σαρωτών.

Για παράδειγμα, με το σαρωτή USB που χρησιμοποιείται στο Διασύνδεση USB, η εντολή `sane-find-scanner` δίνει τις ακόλουθες πληροφορίες:

```
# sane-find-scanner -q
found USB scanner (UNKNOWN vendor and product) at device /dev/uscanner0
```

Ο σαρωτής βρέθηκε, χρησιμοποιεί διασύνδεση USB και το όνομα συσκευής του είναι /dev/uscanner0. Τώρα πρέπει να δούμε αν αναγνωρίζεται και σωστά:

```
# scanimage -L

No scanners were identified. If you were expecting something different,
check that the scanner is plugged in, turned on and detected by the
sane-find-scanner tool (if appropriate). Please read the documentation
which came with this software (README, FAQ, manpages).
```

Αφού ο σαρωτής δεν αναγνωρίστηκε, θα χρειαστεί να επεξεργαστούμε το αρχείο /usr/local/etc/sane.d/epson2.conf. Το μοντέλο σαρωτή που χρησιμοποιήθηκε ήταν το EPSON Perfection® 1650, έτσι ξέρουμε ότι ο σαρωτής θα χρησιμοποιεί το backend `epson2`. Βεβαιωθείτε ότι διαβάσατε τα βοηθητικά σχόλια στα αρχεία ρυθμίσεων του backend. Είναι αρκετά απλό να αλλάξετε γραμμές: Μετατρέψτε σε σχόλια όσες γραμμές δείχνουν λάθος τύπο διασύνδεσης για το σαρωτή σας (στην περίπτωση μας θα μετατρέψουμε σε σχόλια όλες τις γραμμές που ξεκινάνε με τη λέξη `scsi` καθώς ο σαρωτής μας χρησιμοποιεί διασύνδεση USB), και προσθέστε στο τέλος του αρχείου μια γραμμή που να ορίζει το είδος διασύνδεσης και το όνομα συσκευής που χρησιμοποιείτε. Στην περίπτωση μας προσθέσαμε την ακόλουθη γραμμή:

```
usb /dev/uscanner0
```

Σας παρακαλούμε να βεβαιωθείτε ότι διαβάσατε τα σχόλια που παρέχονται στο αρχείο ρυθμίσεων του backend καθώς και στις αντίστοιχες σελίδες manual για περισσότερες λεπτομέρειες καθώς και για τη σύνταξη που πρέπει να χρησιμοποιήσετε. Μπορούμε τώρα να επιβεβαιώσουμε ότι ο σαρωτής αναγνωρίζεται:

```
# scanimage -L
device `epson:/dev/uscanner0' is a Epson GT-8200 flatbed scanner
```

Ο USB σαρωτής μας αναγνωρίστηκε. Δεν είναι σημαντικό ότι η μάρκα και το μοντέλο δεν ταιριάζουν ακριβώς με το δικό μας. Το βασικό σημείο είναι το πεδίο `epson:/dev/uscanner0'`, το οποίο δείχνει το σωστό backend και όνομα συσκευής.

Μόλις η εντολή `scanimage -L` μπορέσει να δει το σαρωτή, η ρύθμιση έχει ολοκληρωθεί. Η συσκευή είναι έτοιμη να χρησιμοποιηθεί.

Αν και η sane(1) μας επιτρέπει να σαρώσουμε εικόνα από τη γραμμή εντολών, είναι προτιμότερο να χρησιμοποιήσουμε κάποιο πρόγραμμα σε γραφικό περιβάλλον για την εργασία αυτή. Το SANE μας προσφέρει ένα απλό αλλά αποδοτικό γραφικό περιβάλλον: το xscanimage (graphics/sane-frontends).

Το Xsane (graphics/xsane) είναι επίσης ένα δημοφιλές frontend πρόγραμμα σάρωσης. Το frontend αυτό προσφέρει προχωρημένες δυνατότητες, όπως διαφορετικούς τρόπους σάρωσης (φωτοτυπία, fax, κλπ) διόρθωση χρωμάτων, πολλαπλή σάρωση κ.α. Και οι δύο αυτές εφαρμογές διατίθενται επίσης σαν πρόσθετο (plugin) πρόγραμμα για χρήση με το GIMP.

14.7.4. Δίνοντας σε Άλλους Χρήστες Πρόσβαση στο Σαρωτή σας

Όλες οι παραπάνω λειτουργίες έγιναν με τα προνόμια του χρήστη `root`. Μπορεί ωστόσο, να θέλετε να δώσετε πρόσβαση στο σαρωτή σας και σε άλλους χρήστες. Ο χρήστης χρειάζεται άδεια ανάγνωσης και εγγραφής στο αρχείο συσκευής που χρησιμοποιείται από το σαρωτή. Σαν παράδειγμα, ο σαρωτής μας χρησιμοποιεί το αρχείο συσκευής /dev/ugen0.2 το οποίο στην πραγματικότητα είναι ένας συμβολικός δεσμός προς το πραγματικό αρχείο συσκευής, το /dev/usb/0.2.0 (μπορείτε να το επιβεβαιώσετε εύκολα με μια ματιά στον κατάλογο /dev). Τόσο ο συμβολικός δεσμός όσο και το αρχείο συσκευής ανήκουν στις ομάδες `wheel` και `operator`. Αν προσθέσουμε το χρήστη `joe` σε αυτές τις ομάδες, θα μπορεί να χρησιμοποιήσει το σαρωτή. Για λόγους ασφαλείας όμως θα πρέπει να είμαστε ιδιαίτερα προσεκτικοί όταν προσθέτουμε ένα χρήστη σε μια ομάδα, ειδικά αν πρόκειται για την `wheel`. Μια καλύτερη λύση θα ήταν να δημιουργήσουμε μια ομάδα ειδικά για τη χρήση των συσκευών USB, και να επιτρέψουμε πρόσβαση στον σαρωτή στα μέλη της ομάδας αυτής.

Για παράδειγμα, θα χρησιμοποιήσουμε μια ομάδα με το όνομα `usb`. Το πρώτο βήμα είναι η δημιουργία αυτής της ομάδας με τη βοήθεια της εντολής pw(8):

```
# pw groupadd usb
```

Θα πρέπει έπειτα να αλλάξουμε τα δικαιώματα του συμβολικού δεσμού /dev/ugen0.2 και του αρχείου συσκευής /dev/ugen0.2.0 ώστε να είναι προσβάσιμα από την ομάδα `usb` με δυνατότητα εγγραφής (δικαιώματα `0660` ή `0664`). Από προεπιλογή, μόνο ο ιδιοκτήτης αυτών των αρχείων (ο `root`) έχει τα απαραίτητα δικαιώματα εγγραφής. Όλα τα παραπάνω μπορούν να γίνουν με τις παρακάτω γραμμές στο αρχείο /etc/devfs.rules:

```
[system=5]
add path ugen0.2 mode 660 group usb
add path usb/0.2.0 mode 0660 group usb
```

Οι χρήστες του FreeBSD 7.X θα χρειαστούν τις παρακάτω γραμμές, με το σωστό αρχείο συσκευής (τις περισσότερες φορές θα είναι το /dev/uscanner0):

```
[system=5]
add path uscanner0 mode 0660 group usb
```

Έπειτα, προσθέστε την ακόλουθη γραμμή στο αρχείο /etc/rc.conf και επανεκκινήστε το μηχάνημα:

```
devfs_system_ruleset="system"
```

Περισσότερες πληροφορίες σχετικά με αυτές τις γραμμές, μπορείτε να βρείτε στη σελίδα manual του devfs(8).

Έπειτα από τα παραπάνω βήματα, για να δώσετε πρόσβαση στο USB σαρωτή σε κάποιο χρήστη, αρκεί να προσθέσετε το λογαριασμό του στην ομάδα `usb`:

```
# pw groupmod usb -m joe
```

Για περισσότερες λεπτομέρειες, διαβάστε τη σελίδα manual του pw(8).

Chapter 15. Ρυθμίζοντας τον Πυρήνα του FreeBSD

15.1. Σύνοψη

Ο πυρήνας είναι η καρδιά του λειτουργικού συστήματος FreeBSD. Είναι υπεύθυνος για τη διαχείριση της μνήμης, την επιβολή των ρυθμίσεων ασφαλείας, τη δικτύωση, την πρόσβαση στο δίσκο, και πολλά άλλα. Ένα συνεχώς αυξανόμενο μέρος του FreeBSD μπορεί να ρυθμιστεί δυναμικά, αλλά υπάρχουν ακόμα περιπτώσεις οι οποίες απαιτούν ρυθμίσεις και μεταγλώττιση του πυρήνα του FreeBSD με προσαρμοσμένες παραμέτρους.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Για ποιους λόγους μπορεί να χρειαστεί να φτιάξετε ένα προσαρμοσμένο πυρήνα.
- Πως να γράψετε ένα αρχείο ρυθμίσεων πυρήνα, ή να αλλάξετε ένα υπάρχον αρχείο ρυθμίσεων.
- Πως να χρησιμοποιήσετε το αρχείο ρυθμίσεων του πυρήνα για να φτιάξετε και να μεταγλωττίσετε ένα νέο πυρήνα.
- Πως να εγκαταστήσετε το νέο πυρήνα.
- Πως να επιλύσετε τυχόν προβλήματα με το νέο πυρήνα.

Όλες οι εντολές που εμφανίζονται σε αυτό το κεφάλαιο ως παραδείγματα πρέπει να εκτελεστούν ως `root` για να είναι επιτυχείς.

15.2. Γιατί να Φτιάξετε Προσαρμοσμένο Πυρήνα;

Κατά παράδοση, το FreeBSD είχε αυτό που αποκαλούμε "μονολιθικό" πυρήνα. Αυτό σημαίνει ότι ο πυρήνας ήταν ένα μεγάλο πρόγραμμα, υποστήριζε ένα σταθερό αριθμό συσκευών, και αν θέλατε να αλλάξετε τη συμπεριφορά του, θα έπρεπε να μεταγλωττίσετε καινούριο και να επανεκκινήσετε τον υπολογιστή σας με αυτόν.

Σήμερα, το FreeBSD κινείται ταχύτατα προς ένα μοντέλο όπου οι περισσότερες λειτουργίες του πυρήνα περιέχονται σε modules (αρθρώματα) τα οποία μπορούν να φορτωθούν και να αποφορτωθούν κατά απαίτηση, δυναμικά στον πυρήνα. Αυτό επιτρέπει στον πυρήνα να προσαρμόζεται σε υλικό το οποίο ενεργοποιείται τη δεδομένη στιγμή (όπως για παράδειγμα όταν εισέρχεται μια κάρτα PCMCIA σε ένα φορητό υπολογιστή). Επίσης επιτρέπει στον πυρήνα να επεκτείνει δυναμικά τη λειτουργικότητά του, προσθέτοντας χαρακτηριστικά τα οποία δεν ήταν απαραίτητα όταν είχε μεταγλωττιστεί αρχικά. Αυτού του είδους ο πυρήνας είναι γνωστός ως modular (αρθρωτός).

Παρ' όλα αυτά, είναι ακόμα απαραίτητο να γίνουν κάποιες στατικές ρυθμίσεις στον πυρήνα. Σε ορισμένες περιπτώσεις, αυτό συμβαίνει επειδή η συγκεκριμένη λειτουργία είναι τόσο στενά συνδεμένη με τον πυρήνα ώστε δεν μπορεί να φορτωθεί δυναμικά. Σε άλλες, συμβαίνει επειδή απλά κανείς δεν έχει ακόμα ασχοληθεί να γράψει ένα δυναμικό module που να παρέχει αυτή τη λειτουργικότητα.

Η δημιουργία προσαρμοσμένου πυρήνα είναι από τις πλέον σημαντικές τελετουργίες κάθε προχωρημένου χρήστη του BSD. Η διαδικασία αυτή, αν και χρονοβόρα, θα αποβεί ιδιαίτερα ωφέλιμη για το FreeBSD σύστημα σας. Σε αντίθεση με τον πυρήνα GENERIC, ο οποίος πρέπει να υποστηρίξει μεγάλο εύρος συσκευών, ένας προσαρμοσμένος πυρήνας περιέχει υποστήριξη μόνο για το υλικό του *δικού σας* υπολογιστή. Έτσι έχετε κάποια οφέλη, όπως:

- Ταχύτερη εκκίνηση. Καθώς ο πυρήνας θα ανιχνεύει μόνο το υλικό που έχετε στο σύστημα σας, ο χρόνος που χρειάζεται για την εκκίνηση του συστήματος σας θα μειωθεί δραματικά.
- Χαμηλότερη κατανάλωση μνήμης. Ένας προσαρμοσμένος πυρήνας, συχνά χρησιμοποιεί λιγότερη μνήμη από τον πυρήνα GENERIC, αφού απουσιάζουν από αυτόν συσκευές και χαρακτηριστικά που δεν χρησιμοποιούνται. Αυτό είναι σημαντικό, καθώς ο πυρήνας βρίσκεται πάντα φορτωμένος στη φυσική μνήμη, μειώνοντας έτσι τη μνήμη που είναι διαθέσιμη για εφαρμογές. Για το λόγο αυτό, ο προσαρμοσμένος πυρήνας είναι ιδιαίτερα χρήσιμος σε συστήματα με μικρό μέγεθος φυσικής μνήμης (RAM).
- Επιπρόσθετη υποστήριξη συσκευών. Ο προσαρμοσμένος πυρήνας σας επιτρέπει να προσθέσετε υποστήριξη για συσκευές οι οποίες δεν υπάρχουν στον GENERIC πυρήνα, όπως για παράδειγμα για κάρτες ήχου.

15.3. Ανακαλύπτοντας τις Συσκευές του Συστήματος σας

Πριν ξεκινήσετε με τη ρύθμιση του πυρήνα σας, θα ήταν σκόπιμο να κάνετε μια απογραφή υλικού του υπολογιστή σας. Σε περιπτώσεις που το FreeBSD δεν είναι το βασικό σας λειτουργικό σύστημα, μπορείτε εύκολα να δημιουργήσετε αυτή τη λίστα, εξετάζοντας τις ρυθμίσεις του τρέχοντος λειτουργικού συστήματος. Για παράδειγμα, η Διαχείριση Συσκευών (Device Manager) της Microsoft® δείχνει συνήθως σημαντικές πληροφορίες σχετικά με τις εγκατεστημένες συσκευές. Μπορείτε να βρείτε την Διαχείριση Συσκευών στον πίνακα ελέγχου.

Μερικές εκδόσεις των Microsoft® Windows® διαθέτουν ένα εικονίδιο με τίτλο Σύστημα (System). Από την οθόνη που εμφανίζεται μπορείτε να επιλέξετε την Διαχείριση Συσκευών.

Αν δεν υπάρχει άλλο λειτουργικό σύστημα στον υπολογιστή, ο διαχειριστής θα πρέπει να βρει αυτές τις πληροφορίες χειροκίνητα. Μια μέθοδος είναι με τη χρήση του βοηθητικού προγράμματος dmesg(8) και της εντολής man(1). Τα περισσότερα προγράμματα οδήγησης του FreeBSD διαθέτουν σελίδα manual, η οποία δείχνει το υποστηριζόμενο υλικό. Κατά τη διάρκεια της εκκίνησης, εμφανίζεται μια λίστα με τις συσκευές που ανιχνεύθηκαν. Για παράδειγμα, οι παρακάτω γραμμές δείχνουν ότι το πρόγραμμα οδήγησης psm εντόπισε ένα ποντίκι:

```
psm0: <PS/2 Mouse> irq 12 on atkbdc0
psm0: [GIANT-LOCKED]
psm0: [ITHREAD]
psm0: model Generic PS/2 mouse, device ID 0
```

Αυτό το πρόγραμμα οδήγησης θα πρέπει να περιληφθεί στο αρχείο ρυθμίσεων του προσαρμοσμένου πυρήνα σας, ή να φορτωθεί δυναμικά μέσω του loader.conf(5).

Σε ορισμένες περιπτώσεις, η έξοδος της `dmesg` μπορεί να δείχνει μόνο τα μηνύματα του συστήματος και όχι τα αποτελέσματα της ανίχνευσης συσκευών. Στις περιπτώσεις αυτές, μπορείτε να δείτε την επιθυμητή έξοδο στα περιεχόμενα του αρχείου /var/run/dmesg.boot.

Μια άλλη μέθοδος για την ανίχνευση του υλικού, είναι μέσω του βοηθητικού προγράμματος pciconf(8), το οποίο παρέχει πιο αναλυτική περιγραφή. Για παράδειγμα:

```
ath0@pci0:3:0:0:        class=0x020000 card=0x058a1014 chip=0x1014168c rev=0x01
hdr=0x00
vendor     = 'Atheros Communications Inc.'
device     = 'AR5212 Atheros AR5212 802.11abg wireless'
class      = network
subclass   = ethernet
```

Η παραπάνω έξοδος, που λήφθηκε μέσω της εντολής `pciconf -lv`, δείχνει ότι το πρόγραμμα οδήγησης ath εντόπισε μια συσκευή ασύρματου Ethernet. Μπορείτε να δείτε την αντίστοιχη σελίδα manual του προγράμματος ath(4), χρησιμοποιώντας την εντολή `man ath`.

Μπορείτε επίσης να πάρετε χρήσιμες πληροφορίες από την εντολή man(1), αν δώσετε την επιλογή `-k`. Στο παραπάνω παράδειγμα, δίνοντας:

```
....`Atheros`
....
```

Θα δείτε μια λίστα από σελίδες manual που περιέχουν τη συγκεκριμένη λέξη:

```
ath(4)                  - Atheros IEEE 802.11 wireless network driver
ath_hal(4)              - Atheros Hardware Access Layer (HAL)
```

Έχοντας διαθέσιμη την απογραφή υλικού του υπολογιστή σας, η διαδικασία δημιουργίας προσαρμοσμένου πυρήνα σίγουρα φαίνεται λιγότερο αποθαρρυντική.

15.4. Προγράμματα Οδήγησης, Υποσυστήματα και Αρθρώματα (modules)

Πριν δημιουργήσετε ένα προσαρμοσμένο πυρήνα, θα πρέπει πρώτα να σκεφτείτε για ποιους λόγους τον χρειάζεστε. Σε πολλές περιπτώσεις, η υποστήριξη κάποιας συγκεκριμένης συσκευής μπορεί να επιτευχθεί με την χρήση κάποιου αρθρώματος (module).

Τα αρθρώματα του πυρήνα βρίσκονται στον κατάλογο /boot/kernel/ και μπορούν να φορτωθούν δυναμικά στον πυρήνα που εκτελείται τη δεδομένη στιγμή, με τη χρήση της εντολής kldload(8). Τα περισσότερα, αν και όχι όλα, τα προγράμματα οδήγησης στον πυρήνα, διατίθενται και σε μορφή αρθρώματος· έχουν επίσης τη δική του σελίδα βοήθειας το καθένα. Για παράδειγμα, στην προηγούμενη ενότητα, είδαμε το πρόγραμμα οδήγησης ασύρματου Ethernet ath. Η σελίδα βοήθειας για αυτή τη συσκευή αναφέρει:

```
Alternatively, to load the driver as a module at boot time, place the
following line in man:loader.conf[5]:

      if_ath_load="YES"
```

Όπως αναφέρεται στις οδηγίες, αν βάλετε την γραμμή `if_ath_load="YES"` στο αρχείο /boot/loader.conf, το άρθρωμα θα φορτωθεί δυναμικά κατά την εκκίνηση του συστήματος σας.

Σε μερικές περιπτώσεις ωστόσο, δεν υπάρχει άρθρωμα που να σχετίζεται με κάποιο πρόγραμμα οδήγησης. Αυτό ισχύει περισσότερο για κάποια ιδιαίτερα υποσυστήματα και πολύ σημαντικά προγράμματα οδήγησης. Για παράδειγμα, το πρόγραμμα οδήγησης του συστήματος αρχείων fast file system (FFS) απαιτείται να είναι ενσωματωμένο στον πυρήνα. Το ίδιο συμβαίνει και με την υποστήριξη δικτύου (INET). Δυστυχώς, ο μόνος τρόπος για να δείτε αν ένα πρόγραμμα οδήγησης πρέπει να είναι υποχρεωτικά ενσωματωμένο στον πυρήνα, είναι να ελέγξετε αν υπάρχει το αντίστοιχο άρθρωμα.

Είναι αρκετά εύκολο να αφαιρέσετε την υποστήριξη για κάποια συσκευή ή άλλη επιλογή, και να καταλήξετε με ένα πυρήνα που δεν μπορεί να ξεκινήσει. Για παράδειγμα, αν βγάλετε το πρόγραμμα οδήγησης ata(4) από το αρχείο ρυθμίσεων του πυρήνα σας, αν το σύστημα σας χρησιμοποιεί δίσκους ATA δεν θα μπορεί να ξεκινήσει. Στην περίπτωση αυτή θα πρέπει να βάλετε την αντίστοιχη γραμμή στο αρχείο loader.conf για να φορτώσετε το σχετικό άρθρωμα. Αν δεν είστε σίγουροι, ελέγξτε για την ύπαρξη του αρθρώματος και απλώς αφήστε την υποστήριξη ενσωματωμένη στον πυρήνα.

15.5. Δημιουργία και Εγκατάσταση Προσαρμοσμένου Πυρήνα

Χρειάζεται να έχετε εγκαταστήσει όλο τον πηγαίο κώδικα του FreeBSD για να μεταγλωττίσετε τον πυρήνα.

Αρχικά, θα κάνουμε μια γρήγορη παρουσίαση του καταλόγου στον οποίο γίνεται η μεταγλώττιση του πυρήνα. Όλοι οι κατάλογοι που θα αναφέρουμε βρίσκονται κάτω από τον κατάλογο /usr/src/sys ο οποίος είναι επίσης προσβάσιμος μέσω της διαδρομής /sys. Υπάρχει εδώ ένας αριθμός υποκαταλόγων ο οποίος αντιπροσωπεύει διαφορετικά τμήματα του πυρήνα, αλλά οι πλέον σημαντικοί για το σκοπό μας είναι οι arch/conf, όπου θα επεξεργαστείτε τις ρυθμίσεις για τον προσαρμοσμένο πυρήνα σας, και ο compile, που είναι ο χώρος εργασίας στον οποίο θα γίνει η μεταγλώττιση του. Ο *arch* αντιπροσωπεύει ένα από τα i386, amd64, ia64, powerpc, sparc64, ή pc98 (ένας εναλλακτικός τύπος PC, διαδεδομένος στην Ιαπωνία). Οτιδήποτε βρίσκεται μέσα στον συγκεκριμένο κατάλογο μιας αρχιτεκτονικής, σχετίζεται μόνο με την αρχιτεκτονική αυτή. Το υπόλοιπο του κώδικα, είναι ανεξάρτητο από την αρχιτεκτονική και κοινό σε κάθε πλατφόρμα όπου θα μπορούσε να μεταγλωττιστεί το FreeBSD. Παρατηρήστε τη λογική οργάνωση της δομής των καταλόγων, όπου κάθε υποστηριζόμενη συσκευή, σύστημα αρχείων και επιλογή βρίσκεται στο δικό της κατάλογο.

Στα παραδείγματα αυτού του κεφαλαίου υποθέτουμε ότι χρησιμοποιείτε την αρχιτεκτονική i386. Αν

χρησιμοποιείτε διαφορετική αρχιτεκτονική, θα χρειαστεί να αλλάξετε τα ονόματα των καταλόγων και διαδρομών ώστε να συμβαδίζουν με αυτή.

Αν δεν υπάρχει ο κατάλογος /usr/src/ στο σύστημα σας (ή αν είναι άδειος), τότε δεν έχετε εγκαταστήσει τον πηγαίο κώδικα. Ο ευκολότερος τρόπος για να εγκαταστήσετε τον πλήρη πηγαίο κώδικα, είναι να μέσω του csup(1) όπως περιγράφεται στο Συγχρονίζοντας τον Πηγαίο σας Κώδικα. Θα πρέπει επίσης να δημιουργήσετε ένα συμβολικό δεσμό προς τον κατάλογο /usr/src/sys/:

```
# ln -s /usr/src/sys /sys
```

Έπειτα, μετακινηθείτε στον κατάλογο arch/conf και αντιγράψτε το αρχείο ρυθμίσεων GENERIC στο όνομα το οποίο θέλετε να δώσετε στο νέο σας πυρήνα. Για παράδειγμα:

```
# cd /usr/src/sys/i386/conf
# cp GENERIC MYKERNEL
```

Κατά παράδοση, το όνομα αυτό γράφεται εξ' ολοκλήρου με κεφαλαία γράμματα και αν έχετε πολλά μηχανήματα FreeBSD με διαφορετικό υλικό, είναι καλή ιδέα να του δώσετε το όνομα του μηχανήματος. Για το παράδειγμα μας, θα το αποκαλούμε MYKERNEL.

Δεν είναι γενικά καλή ιδέα να αποθηκεύσετε το αρχείο ρυθμίσεων σας απευθείας στον κατάλογο /usr/src. Αν αντιμετωπίσετε προβλήματα, ίσως μπείτε στον πειρασμό να διαγράψετε απλώς τον κατάλογο /usr/src και να ξεκινήσετε από την αρχή. Συνήθως λίγα δευτερόλεπτα μετά από αυτό θα συνειδητοποιήσετε ότι έχετε επίσης διαγράψει το αρχείο ρυθμίσεων του πυρήνα σας. Επίσης, μην επεξεργάζεστε απευθείας το αρχείο GENERIC, καθώς μπορεί οι αλλαγές σας να χαθούν την επόμενη φορά που θα ανανεώσετε τον πηγαίο σας κώδικα.

Καλό θα είναι να αποθηκεύσετε το αρχείο ρυθμίσεων σε άλλο κατάλογο και να δημιουργήσετε ένα συμβολικό δεσμό προς το αρχείο, στον κατάλογο i386.

Για παράδειγμα:

```
# cd /usr/src/sys/i386/conf
# mkdir /root/kernels
# cp GENERIC /root/kernels/MYKERNEL
# ln -s /root/kernels/MYKERNEL
```

Τώρα, τροποποιήστε το αρχείο MYKERNEL με τον επεξεργαστή κειμένου που προτιμάτε. Αν ξεκινάτε μόλις τώρα, πιθανόν ο μόνος διαθέσιμος επεξεργαστής κειμένου να είναι το vi, ο οποίος είναι αρκετά πολύπλοκος για να τον εξηγήσουμε εδώ, αλλά καλύπτεται αρκετά καλά από πλήθος βιβλίων στην βιβλιογραφία. Ωστόσο, το FreeBSD διαθέτει επίσης ένα ευκολότερο επεξεργαστή κειμένου, τον ee ο οποίος είναι η κατάλληλη επιλογή αν είστε αρχάριος. Αλλάξτε κατά βούληση τα σχόλια στην αρχή του αρχείου ρυθμίσεων ώστε να αντανακλούν τις αλλαγές που έχετε κάνει και οι

οποίες το διαχωρίζουν από το GENERIC.

Αν έχετε δημιουργήσει πυρήνα στο SunOS™ ή σε κάποιο άλλο λειτουργικό σύστημα τύπου BSD, το μεγαλύτερο μέρος αυτού του αρχείου θα σας φανεί γνωστό. Από την άλλη, αν έρχεστε από κάποιο άλλο λειτουργικό, όπως το DOS το αρχείο ρυθμίσεων GENERIC ίσως να σας είναι δύσκολο στην κατανόηση, για το λόγο αυτό ακολουθήστε αργά και προσεκτικά τις περιγραφές του τμήματος Αρχείο Ρυθμίσεων.

Αν συγχρονίσετε τον πηγαίο κώδικα με τις τελευταίες αλλαγές του FreeBSD project, να διαβάσετε το αρχείο /usr/src/UPDATING πριν προχωρήσετε σε οποιοδήποτε βήμα αναβάθμισης. Το αρχείο αυτό περιγράφει πιθανά σημαντικά προβλήματα ή περιοχές που χρειάζονται ιδιαίτερη προσοχή όσο αφορά τον ανανεωμένο πηγαίο κώδικα. Το αρχείο /usr/src/UPDATING ταιριάζει πάντα με την έκδοση του πηγαίου κώδικα του FreeBSD που έχετε, και είναι για αυτό το λόγο πιο ενημερωμένο σε σχέση με ότι διαβάσετε στο παρόν βιβλίο.

Θα πρέπει τώρα να μεταγλωττίσετε τον πηγαίο κώδικα του πυρήνα.

Procedure: Μεταγλώττιση του Πυρήνα

Χρειάζεται να έχετε εγκαταστήσει όλο τον πηγαίο κώδικα του FreeBSD για να μεταγλωττίσετε τον πυρήνα.

1. Μετακινηθείτε στον κατάλογο /usr/src:

```
# cd /usr/src
```

2. Μεταγλωττίστε τον πυρήνα:

```
# make buildkernel KERNCONF=MYKERNEL
```

3. Εγκαταστήστε το νέο πυρήνα:

```
# make installkernel KERNCONF=MYKERNEL
```

Από προεπιλογή, όταν δημιουργείτε ένα προσαρμοσμένο πυρήνα, δημιουργούνται επίσης και *όλα* τα modules (αρθρώματα) πυρήνα. Αν θέλετε να κάνετε πιο γρήγορη ανανέωση του πυρήνα ή να δημιουργήσετε μόνο συγκεκριμένα modules, θα πρέπει να τροποποιήσετε το αρχείο /etc/make.conf πριν ξεκινήσετε τη δημιουργία του πυρήνα:

```
MODULES_OVERRIDE = linux acpi sound/sound sound/driver/ds1 ntfs
```

Στη μεταβλητή αυτή δίνετε μια λίστα των modules που θέλετε να δημιουργηθούν, αντί να δημιουργηθούν όλα.

```
WITHOUT_MODULES = linux acpi sound ntfs
```

Στη μεταβλητή αυτή δίνετε μια λίστα βασικών (top level) modules που θέλετε να παραλείψετε κατά τη διαδικασία δημιουργίας. Για άλλες μεταβλητές που ίσως είναι χρήσιμες στη διαδικασία δημιουργίας πυρήνα, δείτε τη σελίδα manual του make.conf(5).

Ο νέος πυρήνας θα αντιγραφεί στον κατάλογο /boot/kernel με το όνομα /boot/kernel/kernel ενώ ο παλιός πυρήνας θα μετακινηθεί στο /boot/kernel.old/kernel. Τερματίστε τώρα το σύστημα σας και επανεκκινήστε για να χρησιμοποιήσετε το νέο πυρήνα. Αν κάτι πάει στραβά, υπάρχουν κάποιες πληροφορίες για Αντιμετώπιση Προβλημάτων που ίσως σας φανούν χρήσιμες, στο τέλος αυτού του κεφαλαίου. Βεβαιωθείτε ότι διαβάσατε το τμήμα που εξηγεί πως να επαναφέρετε το σύστημα σας σε περίπτωση που ο νέος πυρήνας δεν εκκινεί.

Άλλα αρχεία που σχετίζονται με τη διαδικασία εκκίνησης, όπως ο loader(8) και οι ρυθμίσεις του, βρίσκονται στον κατάλογο /boot. Εξειδικευμένα modules ή modules τρίτων κατασκευαστών μπορούν να τοποθετηθούν στον κατάλογο /boot/kernel, αν και οι χρήστες θα πρέπει να γνωρίζουν ότι είναι σημαντικό τα modules να είναι σε συγχρονισμό με τον πυρήνα. Modules τα οποία δεν προορίζονται για εκτέλεση με τον τρέχοντα πυρήνα, μπορούν να προκαλέσουν αστάθεια ή εσφαλμένη λειτουργία του συστήματος σας.

15.6. Το Αρχείο Ρυθμίσεων

Η γενική μορφή ενός αρχείου ρυθμίσεων πυρήνα, είναι αρκετά απλή. Κάθε γραμμή περιέχει μια λέξη-κλειδί και ένα ή περισσότερα ορίσματα. Για λόγους απλότητας, οι περισσότερες γραμμές περιέχουν μόνο ένα όρισμα. Οτιδήποτε βρίσκεται μετά το σύμβολο # θεωρείται σχόλιο και αγνοείται. Στα επόμενα τμήματα θα βρείτε περιγραφή για τις λέξεις-κλειδιά, με τη σειρά που εμφανίζονται στο αρχείο ρυθμίσεων GENERIC. Για εξαντλητική λίστα των παραμέτρων και συσκευών που εξαρτώνται από την αρχιτεκτονική, δείτε το αρχείο NOTES το οποίο βρίσκεται στον ίδιο κατάλογο με το αρχείο GENERIC. Για επιλογές και ρυθμίσεις που είναι ανεξάρτητες από την αρχιτεκτονική, δείτε το αρχείο /usr/src/sys/conf/NOTES.

Μπορείτε να χρησιμοποιήσετε την οδηγία `include` στα αρχεία ρυθμίσεων. Η οδηγία αυτή επιτρέπει την λογική συμπερίληψη ενός άλλου αρχείου ρυθμίσεων μέσα στο τρέχον, κάνοντας πιο εύκολη τη συντήρηση του όταν οι αλλαγές που χρειάζονται είναι λίγες σε σχέση με το αρχικό αρχείο. Για παράδειγμα, αν χρειάζεστε ένα πυρήνα GENERIC με λίγες μόνο παραπάνω επιλογές ή προγράμματα οδήγησης, μπορείτε να δημιουργήσετε ένα μικρό αρχείο διαφορών σε σχέση με τον GENERIC:

```
include GENERIC
ident MYKERNEL

options         IPFIREWALL
```

```
options         DUMMYNET
options         IPFIREWALL_DEFAULT_TO_ACCEPT
options         IPDIVERT
```

Πολλοί διαχειριστές βρίσκουν ότι αυτό το μοντέλο προσφέρει σημαντικά πλεονεκτήματα σε σχέση με τον παραδοσιακό τρόπο συγγραφής αρχείων ρυθμίσεων από το μηδέν: το τοπικό αρχείο ρυθμίσεων περιέχει μόνο τις διαφορές από ένα πυρήνα GENERIC. Καθώς γίνονται αναβαθμίσεις στο σύστημα, τα νέα χαρακτηριστικά και δυνατότητες που προστίθενται στον GENERIC θα προστεθούν και στον προσαρμοσμένο πυρήνα, εκτός αν το αποτρέψετε χρησιμοποιώντας το `nooptions` ή το `nodevice`. Το υπόλοιπο αυτού του κεφαλαίου, εξηγεί το περιεχόμενο ενός τυπικού αρχείου ρυθμίσεων και το ρόλο που έχουν οι διάφορες επιλογές και τα προγράμματα οδήγησης που εμφανίζονται σε αυτό.

Για να δημιουργήσετε ένα αρχείο το οποίο να περιέχει όλες τις διαθέσιμες επιλογές, όπως γίνεται συνήθως για δοκιμές, εκτελέστε την ακόλουθη εντολή ως `root`:

```
# cd /usr/src/sys/i386/conf && make LINT
```

Το παρακάτω είναι ένα παράδειγμα του αρχείου ρυθμίσεων GENERIC με επιπρόσθετα διευκρινιστικά σχόλια όπου είναι απαραίτητο. Το παράδειγμα θα πρέπει να ταιριάζει αρκετά καλά με το αντίγραφο του αρχείου πού έχετε στο /usr/src/sys/i386/conf/GENERIC.

```
machine     i386
```

Πρόκειται για την αρχιτεκτονική του μηχανήματος. Πρέπει να είναι `amd64`, `i386`, `ia64`, `pc98`, `powerpc`, ή `sparc64`.

```
cpu         I486_CPU
cpu         I586_CPU
cpu         I686_CPU
```

Η παραπάνω επιλογή καθορίζει τον τύπο της CPU που έχετε στο σύστημα σας. Μπορεί να έχετε παραπάνω από μια τέτοιες γραμμές (αν για παράδειγμα δεν είστε σίγουρος αν θα πρέπει να χρησιμοποιήσετε `I586_CPU` ή `I686_CPU`), αλλά για ένα προσαρμοσμένο πυρήνα είναι καλύτερα να καθορίσετε μόνο τη CPU που έχετε. Αν δεν είστε σίγουρος για τον τύπο της CPU μπορείτε να ελέγξετε το αρχείο /var/run/dmesg.boot για να δείτε τα μηνύματα εκκίνησης του συστήματος σας.

```
ident         GENERIC
```

Αυτό είναι το αναγνωριστικό όνομα του πυρήνα. Θα πρέπει να το αλλάξετε στο όνομα που δώσατε στον πυρήνα σας, π.χ. `MYKERNEL` αν έχετε ακολουθήσει τις οδηγίες από το προηγούμενο μας παράδειγμα. Η τιμή που θα βάλετε στο αλφαριθμητικό `ident` θα εκτυπώνεται όταν εκκινείτε με τον συγκεκριμένο πυρήνα, και έτσι είναι χρήσιμο να δώσετε στο νέο πυρήνα ένα διαφορετικό όνομα αν θέλετε να το ξεχωρίζετε από το συνηθισμένο πυρήνα σας (αν π.χ. θέλετε να φτιάξετε ένα

πειραματικό πυρήνα).

```
#To statically compile in device wiring instead of /boot/device.hints
#hints          "GENERIC.hints"         # Default places to look for devices.
```

Το αρχείο device.hints(5) χρησιμοποιείται για τον καθορισμό επιλογών που σχετίζονται με τους οδηγούς συσκευών. Η προεπιλεγμένη θέση την οποία ελέγχει ο loader(8) κατά την εκκίνηση είναι το /boot/device.hints. Χρησιμοποιώντας την επιλογή `hints` μπορείτε να ενσωματώσετε στατικά τις οδηγίες αυτές μέσα στον πυρήνα. Στην περίπτωση αυτή δεν υπάρχει λόγος να δημιουργήσετε το αρχείο device.hints στον κατάλογο /boot.

```
makeoptions     DEBUG=-g          # Build kernel with gdb(1) debug symbols
```

Η φυσιολογική διαδικασία δημιουργίας του FreeBSD περιλαμβάνει πληροφορίες εκσφαλμάτωσης (debugging) όταν ο πυρήνας δημιουργείται με την επιλογή `-g`, επιτρέποντας έτσι την χρήση τους όταν δοθούν στο gcc(1).

```
options         SCHED_ULE         # ULE scheduler
```

Ο προεπιλεγμένος scheduler του FreeBSD. Κρατήστε την επιλογή αυτή.

```
options         PREEMPTION         # Enable kernel thread preemption
```

Επιτρέπει σε νήματα του πυρήνα να προσπεραστούν από άλλα, υψηλότερης προτεραιότητας. Βοηθάει στην αύξηση απόκρισης του συστήματος και επιτρέπει σε νήματα διακοπών (interrupts) να εκτελεστούν πιο γρήγορα, αντί να μένουν σε αναμονή.

```
options         INET              # InterNETworking
```

Υποστήριξη δικτύου. Αφήστε την επιλογή αυτή ενεργοποιημένη, ακόμα και αν δεν σκοπεύετε να συνδεθείτε σε κάποιο δίκτυο. Τα περισσότερα προγράμματα χρειάζονται έστω και την εσωτερική (loopback) δικτύωση (τη δυνατότητα δηλ. να κάνουν συνδέσεις δικτύου μέσα στο ίδιο σας το μηχάνημα), καθιστώντας την επιλογή αυτή ουσιαστικά υποχρεωτική.

```
options         INET6             # IPv6 communications protocols
```

Η επιλογή αυτή ενεργοποιεί τα πρωτόκολλα επικοινωνίας IPv6.

```
options         FFS               # Berkeley Fast Filesystem
```

Πρόκειται για το βασικό σύστημα αρχείων του σκληρού δίσκου. Αφήστε την επιλογή αυτή ενεργοποιημένη, αν ξεκινάτε από το σκληρό δίσκο.

```
options         SOFTUPDATES       # Enable FFS Soft Updates support
```

Η επιλογή αυτή ενεργοποιεί τα Soft Updates στον πυρήνα, το οποίο βοηθάει την επιτάχυνση της εγγραφής στους δίσκους. Ακόμα και αν η λειτουργία αυτή παρέχεται από τον πυρήνα, θα πρέπει επίσης να ενεργοποιηθεί για συγκεκριμένους δίσκους. Δείτε την έξοδο της εντολής mount(8) για να δείτε αν είναι ενεργοποιημένα τα Soft Updates στους δίσκους του συστήματος σας. Αν δεν δείτε την επιλογή `soft-updates` θα χρειαστεί να την ενεργοποιήσετε με την εντολή tunefs(8) (για υπάρχοντα συστήματα αρχείων) ή newfs(8) (για νέα συστήματα αρχείων).

```
options         UFS_ACL           # Support for access control lists
```

Με την επιλογή αυτή, ενεργοποιείται η υποστήριξη του πυρήνα για λίστες ελέγχου πρόσβασης (access control lists). Τα ACLs εξαρτιούνται από τη χρήση εκτεταμένων ιδιοτήτων και από το σύστημα αρχείων UFS2, και περιγράφονται με λεπτομέρεια στο File System Access Control Lists. Τα ACLs είναι ενεργοποιημένα από προεπιλογή, και δεν θα πρέπει να τα απενεργοποιήσετε από τον πυρήνα αν έχουν χρησιμοποιηθεί στο παρελθόν σε κάποιο σύστημα αρχείων, καθώς αυτό θα τα αφαιρέσει από τα αρχεία, αλλάζοντας έτσι τον τρόπο προστασίας τους με απρόβλεπτους τρόπους.

```
options         UFS_DIRHASH       # Improve performance on big directories
```

Με την επιλογή αυτή, περιλαμβάνονται λειτουργίες που αυξάνουν την ταχύτητα πρόσβασης του δίσκου σε μεγάλους καταλόγους, με κόστος τη χρήση επιπρόσθετης μνήμης. Φυσιολογικά, θα θέλετε να κρατήσετε την επιλογή αυτή σε ένα μεγάλο εξυπηρετητή ή σταθμό εργασίας, και να την αφαιρέσετε όταν χρησιμοποιείτε το FreeBSD σε ένα μικρό σύστημα όπου η μνήμη είναι περιορισμένη και η ταχύτητα πρόσβασης στο δίσκο είναι λιγότερο σημαντική, όπως για παράδειγμα σε ένα firewall.

```
options         MD_ROOT           # MD is a potential root device
```

Με την επιλογή αυτή ενεργοποιείται η υποστήριξη χρήσης ενός εικονικού δίσκου στη μνήμη RAM (ramdrive) για χρήση ως συσκευή root.

```
options         NFSCLIENT         # Network Filesystem Client
options         NFSSERVER         # Network Filesystem Server
options         NFS_ROOT          # NFS usable as /, requires NFSCLIENT
```

Το δικτυακό σύστημα αρχείων. Αν δεν έχετε σκοπό να προσαρτήσετε συστήματα αρχείων από άλλο εξυπηρετητή αρχείων UNIX® μέσω TCP/IP, μπορείτε να μετατρέψετε αυτές τις γραμμές σε σχόλια.

```
options         MSDOSFS           # MSDOS Filesystem
```

Το σύστημα αρχείων του MS-DOS®. Αν δεν σκοπεύετε να προσαρτήσετε δίσκο DOS κατά την

εκκίνηση, μπορείτε με ασφάλεια να μετατρέψετε την επιλογή αυτή σε σχόλιο. Η υποστήριξη θα φορτωθεί αυτόματα την πρώτη φορά που θα προσαρτήσετε κατάτμηση DOS όπως περιγράψαμε παραπάνω. Επίσης, το εξαιρετικό πρόγραμμα emulators/mtools σας επιτρέπει να έχετε πρόσβαση σε δισκέτες DOS χωρίς να χρειάζεται να τις προσαρτήσετε και να αποπροσαρτήσετε (και επίσης δεν απαιτεί τη χρήση του MSDOSFS).

```
options         CD9660          # ISO 9660 Filesystem
```

Το σύστημα αρχείων ISO 9660 για CDROM. Μετατρέψτε το σε σχόλιο αν δεν έχετε οδηγό CDROM ή αν σπάνια προσαρτάτε CD δεδομένων (καθώς θα φορτωθεί δυναμικά την πρώτη φορά που θα προσαρτήσετε τέτοιο CD). Τα μουσικά CD δεν χρειάζονται αυτό το σύστημα αρχείων.

```
options         PROCFS          # Process filesystem (requires PSEUDOFS)
```

Αυτό το σύστημα αρχείων περιέχει τις διεργασίες του συστήματος. Πρόκειται για ένα "εικονικό" σύστημα αρχείων το οποίο προσαρτάται στον κατάλογο /proc και επιτρέπει σε προγράμματα όπως το ps(1) να δίνουν περισσότερες πληροφορίες για τις διεργασίες που εκτελούνται. Η χρήση του PROCFS δεν απαιτείται στις περισσότερες περιπτώσεις, καθώς τα περισσότερα εργαλεία παρακολούθησης και εκσφαλμάτωσης έχουν προσαρμοστεί να εκτελούνται χωρίς το PROCFS. Στις νέες εγκαταστάσεις, αυτό το σύστημα αρχείων δεν προσαρτάται από προεπιλογή.

```
options         PSEUDOFS        # Pseudo-filesystem framework
```

Πυρήνες που χρησιμοποιούν το PROCFS πρέπει επίσης να παρέχουν υποστήριξη για το PSEUDOFS.

```
options         GEOM_PART_GPT   # GUID Partition Tables.
```

Προσθέτει υποστήριξη για Πίνακα Κατατμήσεων GUID. Το GPT δίνει δυνατότητα ύπαρξης μεγάλου αριθμού κατατμήσεων στο δίσκο, μέχρι 128 με τις τυπικές ρυθμίσεις.

```
options         COMPAT_43       # Compatible with BSD 4.3 [KEEP THIS!]
```

Συμβατότητα με το 4.3BSD. Αφήστε την επιλογή αυτή ενεργή: κάποια προγράμματα θα συμπεριφέρονται παράξενα αν την απενεργοποιήσετε.

```
options         COMPAT_FREEBSD4 # Compatible with FreeBSD4
```

Η επιλογή αυτή απαιτείται για την υποστήριξη εφαρμογών που έχουν μεταγλωττιστεί σε παλιότερες εκδόσεις του FreeBSD και οι οποίες χρησιμοποιούν παλιές διεπαφές και κλήσεις συστήματος. Συνίσταται να υπάρχει αυτή η επιλογή σε όλα τα συστήματα i386™ τα οποία εκτελούν παλιότερες εφαρμογές. Αρχιτεκτονικές όπως η ia64 και η sparc64 που άρχισαν να υποστηρίζονται από την έκδοση 5.X και μετά δεν χρειάζονται αυτή την επιλογή.

```
options         COMPAT_FREEBSD5   # Compatible with FreeBSD5
```

Η επιλογή αυτή απαιτείται στο για την υποστήριξη εφαρμογών που έχουν μεταγλωττιστεί στο FreeBSD 5.X και χρησιμοποιούν τις αντίστοιχες κλήσεις αυτού του συστήματος.

```
options         COMPAT_FREEBSD6   # Compatible with FreeBSD6
```

Η επιλογή αυτή απαιτείται στο για την υποστήριξη εφαρμογών που έχουν μεταγλωττιστεί στο FreeBSD 6.X και χρησιμοποιούν τις αντίστοιχες κλήσεις αυτού του συστήματος.

```
options         COMPAT_FREEBSD7   # Compatible with FreeBSD75
```

Η επιλογή αυτή απαιτείται στο για την υποστήριξη εφαρμογών που έχουν μεταγλωττιστεί στο FreeBSD 7.X και χρησιμοποιούν τις αντίστοιχες κλήσεις αυτού του συστήματος.

```
options         SCSI_DELAY=5000  # Delay (in ms) before probing SCSI
```

Με την επιλογή αυτή ο πυρήνας περιμένει 5 δευτερόλεπτα πριν ανιχνεύσει κάθε συσκευή SCSI στο σύστημα σας. Αν έχετε μόνο IDE δίσκους μπορείτε να την αγνοήσετε, διαφορετικά μπορείτε να δοκιμάσετε να μειώσετε τον αριθμό αυτό, για να επιταχύνετε την εκκίνηση. Φυσικά, αν το κάνετε αυτό και ανακαλύψετε ότι το FreeBSD έχει πρόβλημα στην αναγνώριση των συσκευών σας, θα πρέπει να την ανεβάσετε ξανά.

```
options         KTRACE           # ktrace(1) support
```

Η επιλογή αυτή ενεργοποιεί το tracing των διεργασιών του πυρήνα, το οποίο είναι χρήσιμο στην εκσφαλμάτωση.

```
options         SYSVSHM          # SYSV-style shared memory
```

Η επιλογή αυτή ενεργοποιεί την κοινόχρηστη μνήμη σύμφωνα με το πρότυπο του System V. Η πλέον κοινή χρήση της, είναι η επέκταση XSHM στα X η οποία χρησιμοποιείται αυτόματα από πολλές βαριές εφαρμογές γραφικών για καλύτερη ταχύτητα. Αν χρησιμοποιείτε X, σίγουρα θέλετε να περιλάβετε αυτή την επιλογή.

```
options         SYSVMSG          # SYSV-style message queues
```

Υποστήριξη για μηνύματα του System V. Η επιλογή αυτή προσθέτει μόνο μερικές εκατοντάδες bytes στον πυρήνα.

```
options         SYSVSEM         # SYSV-style semaphores
```

Υποστήριξη σηματοφορέων του System V. Χρησιμοποιείται λιγότερο συχνά, αλλά προσθέτει μόνο μερικές εκατοντάδες bytes στον πυρήνα.

Η επιλογή `-p` της εντολής ipcs(1) θα σας δείξει ποιες διεργασίες χρησιμοποιούν κάθε μια από αυτές τις λειτουργίες του System V.

```
options         _KPOSIX_PRIORITY_SCHEDULING # POSIX P1003_1B real-time extensions
```

Επεκτάσεις πραγματικού χρόνου (Real-time) που προστέθηκαν στο POSIX® το 1993. Χρησιμοποιείται από κάποιες εφαρμογές στη συλλογή των ports (όπως το StarOffice™).

```
options         KBD_INSTALL_CDEV  # install a CDEV entry in /dev
```

Η επιλογή αυτή είναι απαραίτητη για τη δημιουργία του αρχείου συσκευής πληκτρολογίου στον κατάλογο /dev.

```
options         ADAPTIVE_GIANT    # Giant mutex is adaptive.
```

Το Giant είναι το όνομα ενός συστήματος αμοιβαίου αποκλεισμού (sleep mutex) το οποίο προστατεύει ένα μεγάλο αριθμό πόρων του πυρήνα. Στις μέρες μας, αυτό θεωρείται ανεπίτρεπτο από πλευράς απόδοσης και αντικαθίσταται με κλειδώματα τα οποία προστατεύουν συγκεκριμένους πόρους. Η επιλογή `ADAPTIVE_GIANT` επιτρέπει στο Giant να συμπεριληφθεί στο σετ των mutexes που μπορούν να εκτελεστούν επιλεκτικά. Έτσι, αν ένα νήμα θέλει να κλειδώσει το Giant mutex, αλλά αυτό είναι ήδη κλειδωμένο από ένα νήμα σε μια άλλη CPU, το πρώτο νήμα θα συνεχίσει να εκτελείται, και θα περιμένει για την απελευθέρωση του κλειδώματος. Φυσιολογικά, το νήμα θα επέστρεφε στην κατάσταση ύπνου (sleep) και θα περίμενε για την επόμενη ευκαιρία εκτέλεσης του. Αν δεν είστε σίγουρος, αφήστε αυτή την επιλογή ενεργή.

Σημειώστε ότι από το FreeBSD 8.0-RELEASE και τις επόμενες εκδόσεις, όλα τα mutexes έχουν από προεπιλογή τη δυνατότητα προσαρμογής, εκτός αν έχει επίτηδες γίνει διαφορετική ρύθμιση, χρησιμοποιώντας την επιλογή `NO_ADAPTIVE_MUTEXES` κατά τη μεταγλώττιση. Το Giant έχει επίσης δυνατότητα προσαρμογής πλέον, και έτσι η επιλογή `ADAPTIVE_GIANT` έχει αφαιρεθεί από το αρχείο ρυθμίσεων πυρήνα.

```
device          apic            # I/O APIC
```

Η συσκευή apic επιτρέπει τη χρήση του I/O APIC για την παράδοση των interrupts (διακοπών). Η συσκευή apic μπορεί να χρησιμοποιηθεί τόσο σε πυρήνες για ένα επεξεργαστή (UP) όσο και για πολλαπλούς (SMP), αλλά στη δεύτερη περίπτωση είναι απαραίτητη. Προσθέστε την επιλογή `options SMP` για να έχετε υποστήριξη πολλαπλών επεξεργαστών.

Η συσκευή apic υπάρχει μόνο στην αρχιτεκτονική i386, η γραμμή αυτή δεν θα πρέπει να χρησιμοποιηθεί σε άλλες αρχιτεκτονικές.

```
device          eisa
```

Θα πρέπει να συμπεριλάβετε την επιλογή αυτή αν έχετε μητρική με δίαυλο τύπου EISA. Ενεργοποιείται έτσι η αυτόματη ανίχνευση και ρύθμιση όλων των συσκευών στο δίαυλο EISA.

```
device          pci
```

Θα πρέπει να συμπεριλάβετε αυτή την επιλογή αν έχετε μητρική με δίαυλο PCI. Ενεργοποιείται έτσι η αυτόματη ανίχνευση των καρτών PCI και η επικοινωνία μεταξύ των διαύλων PCI και ISA.

```
# Floppy drives
device          fdc
```

Πρόκειται για τον ελεγκτή μονάδας δισκέτας.

```
# ATA and ATAPI devices
device          ata
```

Αυτός ο οδηγός υποστηρίζει όλες τις συσκευές τύπου ATA και ATAPI. Χρειάζεστε μόνο μια καταχώρηση `device ata` για να ανιχνεύσει ο πυρήνας όλες τις συσκευές ATA/ATAPI τύπου PCI στα σύγχρονα μηχανήματα.

```
device          atadisk                 # ATA disk drives
```

Η επιλογή αυτή απαιτείται μαζί με το `device ata` για την υποστήριξη δίσκων ATA.

```
device          ataraid                 # ATA RAID drives
```

Η επιλογή αυτή απαιτείται μαζί με το `device ata` για την υποστήριξη δίσκων ATA RAID.

```
device          atapicd                 # ATAPI CDROM drives
```

Η επιλογή αυτή απαιτείται μαζί με το `device ata` για την υποστήριξη οδηγών ATAPI CDROM.

```
device          atapifd                 # ATAPI floppy drives
```

Η επιλογή αυτή απαιτείται μαζί με το `device ata` για την υποστήριξη οδηγών δισκέτας ATAPI.

```
device          atapist                 # ATAPI tape drives
```

Η επιλογή αυτή απαιτείται μαζί με το `device ata` για την υποστήριξη μονάδων ταινίας ATAPI.

```
options         ATA_STATIC_ID           # Static device numbering
```

Με την επιλογή αυτή, ο αριθμός του ελεγκτή γίνεται στατικός. Χωρίς αυτή, οι αριθμοί συσκευών αποδίδονται δυναμικά.

```
# SCSI Controllers
device          ahb         # EISA AHA1742 family
device          ahc         # AHA2940 and onboard AIC7xxx devices
options         AHC_REG_PRETTY_PRINT    # Print register bitfields in debug
                                        # output.  Adds ~128k to driver.
device          ahd         # AHA39320/29320 and onboard AIC79xx devices
options         AHD_REG_PRETTY_PRINT    # Print register bitfields in debug
                                        # output.  Adds ~215k to driver.
device          amd         # AMD 53C974 (Teckram DC-390(T))
device          isp         # Qlogic family
#device         ispfw       # Firmware for QLogic HBAs- normally a module
device          mpt         # LSI-Logic MPT-Fusion
#device         ncr         # NCR/Symbios Logic
device          sym         # NCR/Symbios Logic (newer chipsets + those of `ncr')
device          trm         # Tekram DC395U/UW/F DC315U adapters

device          adv         # Advansys SCSI adapters
device          adw         # Advansys wide SCSI adapters
device          aha         # Adaptec 154x SCSI adapters
device          aic         # Adaptec 15[012]x SCSI adapters, AIC-6[23]60.
device          bt          # Buslogic/Mylex MultiMaster SCSI adapters

device          ncv         # NCR 53C500
device          nsp         # Workbit Ninja SCSI-3
device          stg         # TMC 18C30/18C50
```

Ελεγκτές SCSI. Μπορείτε να μετατρέψετε σε σχόλιο οποιονδήποτε δεν έχετε στο σύστημα σας. Αν το σύστημα σας έχει μόνο συσκευές IDE, μπορείτε να αφαιρέσετε όλες τις γραμμές. Οι γραμμές τύπου `*_REG_PRETTY_PRINT` χρησιμοποιούνται για να δίνουν περισσότερες διαγνωστικές πληροφορίες για τους αντίστοιχους οδηγούς.

```
# SCSI peripherals
device          scbus       # SCSI bus (required for SCSI)
device          ch          # SCSI media changers
device          da          # Direct Access (disks)
device          sa          # Sequential Access (tape etc)
device          cd          # CD
```

```
device          pass        # Passthrough device (direct SCSI access)
device          ses         # SCSI Environmental Services (and SAF-TE)
```

Περιφερειακά SCSI. Μπορείτε και πάλι να μετατρέψετε σε σχόλιο όσες συσκευές δεν έχετε, ή αν έχετε μόνο συσκευές IDE, μπορείτε να αφαιρέσετε εντελώς αυτές τις γραμμές.

Ο οδηγός USB umass(4) και κάποιοι άλλοι οδηγοί χρησιμοποιούν το υποσύστημα SCSI αν και δεν είναι πραγματικές SCSI συσκευές. Για το λόγο αυτό, σιγουρευτείτε ότι δεν αφαιρέσατε την υποστήριξη SCSI αν περιλαμβάνονται τέτοιοι οδηγοί στο αρχείο ρύθμισης του πυρήνα σας.

```
# RAID controllers interfaced to the SCSI subsystem
device          amr         # AMI MegaRAID
device          arcmsr      # Areca SATA II RAID
device          asr         # DPT SmartRAID V, VI and Adaptec SCSI RAID
device          ciss        # Compaq Smart RAID 5*
device          dpt         # DPT Smartcache III, IV - See NOTES for options
device          hptmv       # Highpoint RocketRAID 182x
device          hptrr       # Highpoint RocketRAID 17xx, 22xx, 23xx, 25xx
device          iir         # Intel Integrated RAID
device          ips         # IBM (Adaptec) ServeRAID
device          mly         # Mylex AcceleRAID/eXtremeRAID
device          twa         # 3ware 9000 series PATA/SATA RAID

# RAID controllers
device          aac         # Adaptec FSA RAID
device          aacp        # SCSI passthrough for aac (requires CAM)
device          ida         # Compaq Smart RAID
device          mfi         # LSI MegaRAID SAS
device          mlx         # Mylex DAC960 family
device          pst         # Promise Supertrak SX6000
device          twe         # 3ware ATA RAID
```

Υποστηριζόμενοι ελεγκτές RAID. Αν δεν έχετε κανένα από αυτούς, μπορείτε να τους μετατρέψετε σε σχόλια ή να τους αφαιρέσετε εντελώς.

```
# atkbdc0 controls both the keyboard and the PS/2 mouse
device          atkbdc      # AT keyboard controller
```

Ο ελεγκτής πληκτρολογίου (atkbdc) παρέχει υπηρεσίες I/O για πληκτρολόγια τύπου AT και συσκευές κατάδειξης (ποντίκια) τύπου PS/2. Ο ελεγκτής απαιτείται για τη λειτουργία του οδηγού πληκτρολογίου (atkbd) και του οδηγού συσκευής κατάδειξης PS/2 (psm).

```
device          atkbd       # AT keyboard
```

Ο οδηγός atkbd, μαζί με τον ελεγκτή atkbdc, παρέχει πρόσβαση σε πληκτρολόγιο τύπου AT 84 ή

εκτεταμένου AT το οποίο συνδέεται στον ελεγκτή πληκτρολογίου.

```
device          psm         # PS/2 mouse
```

Χρησιμοποιήστε αυτή τη συσκευή αν το ποντίκι σας συνδέεται στην θύρα PS/2.

```
device          kbdmux        # keyboard multiplexer
```

Βασική υποστήριξη πολυπλεξίας πληκτρολογίων. Αν δε σκοπεύετε να χρησιμοποιήσετε περισσότερα από ένα πληκτρολόγια στο σύστημα σας, μπορείτε με ασφάλεια να αφαιρέσετε αυτή τη γραμμή.

```
device          vga         # VGA video card driver
```

Το πρόγραμμα οδήγησης της κάρτας γραφικών.

```
device          splash      # Splash screen and screen saver support
```

Γραφική οθόνη (splash) κατά την εκκίνηση! Η συσκευή αυτή χρησιμοποιείται επίσης από τα προγράμματα προφύλαξης οθόνης (κονσόλας).

```
# syscons is the default console driver, resembling an SCO console
device          sc
```

Ο οδηγός `sc` είναι ο προεπιλεγμένος οδηγός κονσόλας και προσομοιώνει κονσόλα τύπου SCO. Καθώς τα περισσότερα προγράμματα πλήρους οθόνης αποκτούν πρόσβαση στην κονσόλα μέσω κάποιας βιβλιοθήκης βάσης δεδομένων τερματικών όπως το termcap, δεν θα πρέπει να έχει σημασία αν χρησιμοποιήσετε αυτόν τον οδηγό ή τον `vt` ο οποίος είναι συμβατός με κονσόλα `VT220`. Μετά την είσοδο σας στο σύστημα, θέστε την μεταβλητή `TERM` στην τιμή `scoansi` αν κάποια προγράμματα πλήρους οθόνης έχουν πρόβλημα όταν χρησιμοποιείται αυτή η κονσόλα.

```
# Enable this for the pcvt (VT220 compatible) console driver
#device          vt
#options         XSERVER          # support for X server on a vt console
#options         FAT_CURSOR       # start with block cursor
```

Πρόκειται για ένα οδηγό κονσόλας συμβατό με VT220, και με προς τα πίσω συμβατότητα με VT100/102. Λειτουργεί καλά σε κάποιους φορητούς υπολογιστές που έχουν ασυμβατότητα υλικού με τον `sc`. Μετά την είσοδο σας στο σύστημα, θέστε την μεταβλητή `TERM` σε `vt100` ή `vt220`. Ο οδηγός μπορεί επίσης να αποδειχθεί χρήσιμος όταν συνδέεστε σε μεγάλο αριθμό από διαφορετικά μηχανήματα μέσω δικτύου, όπου δεν υπάρχουν καταχωρήσεις για τη συσκευή `sc` στο termcap ή terminfo - το `vt100` θα πρέπει να είναι διαθέσιμο πρακτικά σε κάθε πλατφόρμα.

```
device          agp
```

Συμπεριλάβετε τη συσκευή αυτή αν έχετε AGP κάρτα στο σύστημα σας. Θα ενεργοποιήσετε με αυτό τον τρόπο την υποστήριξη για AGP και AGP GART για μητρικές που υποστηρίζουν αυτές τις λειτουργίες.

```
# Power management support (see NOTES for more options)
#device          apm
```

Υποστήριξη Advanced Power Management (προχωρημένης διαχείρισης ισχύος). Χρήσιμο για φορητά, αν και η επιλογή αυτή, από προεπιλογή, είναι ανενεργή στον πυρήνα GENERIC.

```
# Add suspend/resume support for the i8254.
device          pmtimer
```

Πρόγραμμα οδήγησης μετρητή χρόνου (Timer) για συμβάντα που σχετίζονται με διαχείριση ενέργειας όπως το APM και το ACPI.

```
# PCCARD (PCMCIA) support
# PCMCIA and cardbus bridge support
device          cbb             # cardbus (yenta) bridge
device          pccard          # PC Card (16-bit) bus
device          cardbus         # CardBus (32-bit) bus
```

Υποστήριξη PCMCIA. Την χρειάζεστε αν χρησιμοποιείτε φορητό υπολογιστή.

```
# Serial (COM) ports
device          sio             # 8250, 16[45]50 based serial ports
```

Πρόκειται για τις σειριακές θύρες οι οποίες είναι γνωστές στον κόσμο του MS-DOS®/Windows® ως θύρες COM.

Αν έχετε εσωτερικό μόντεμ στη θύρα COM4 και έχετε και σειριακή θύρα COM2, θα πρέπει να αλλάξετε το IRQ του μόντεμ στο 2 (για περίεργους τεχνικούς λόγους, IRQ2 = IRQ 9) για να μπορέσετε να το χρησιμοποιήσετε από το FreeBSD. Αν έχετε κάρτα πολλαπλών σειριακών εξόδων, ελέγξτε τη σελίδα manual του sio(4) για περισσότερες πληροφορίες σχετικά με τις σωστές τιμές που πρέπει να προσθέσετε στο /boot/device.hints. Κάποιες κάρτες γραφικών (ειδικά αυτές που βασίζονται σε ολοκληρωμένα S3) χρησιμοποιούν διευθύνσεις IO μορφής `0x*2e8`, και καθώς πολλές φτηνές σειριακές κάρτες δεν αποκωδικοποιούν πλήρως τη 16 bit περιοχή διευθύνσεων, συγκρούονται με τις κάρτες αυτές, καθιστώντας έτσι πρακτικά άχρηστη τη θύρα COM4.

Κάθε σειριακή πόρτα χρειάζεται να έχει μια μοναδική IRQ (εκτός αν

χρησιμοποιείτε κάρτα πολλαπλών σειριακών που υποστηρίζει κοινή χρήση interrupts), και έτσι δεν μπορούν να χρησιμοποιηθούν τα προεπιλεγμένα interrupts για την COM3 και την COM4.

```
# Parallel port
device          ppc
```

Πρόκειται για την παράλληλη θύρα στο δίαυλο ISA.

```
device          ppbus      # Parallel port bus (required)
```

Παρέχει υποστήριξη για το δίαυλο της παράλληλης θύρας.

```
device          lpt        # Printer
```

Παρέχει υποστήριξη για εκτυπωτές παράλληλης θύρας.

Χρειάζεστε και τα τρία παραπάνω για να ενεργοποιήσετε την υποστήριξη εκτυπωτή παράλληλης θύρας.

```
device          plip       # TCP/IP over parallel
```

Πρόκειται για το πρόγραμμα οδήγησης δικτύου μέσω παράλληλης θύρας.

```
device          ppi        # Parallel port interface device
```

Πρόγραμμα I/O γενικής χρήσης ("geek port") + IEEE1284 I/O.

```
#device         vpo        # Requires scbus and da
```

Χρησιμοποιείται για μονάδα δισκέτας Iomega Zip. Απαιτεί υποστήριξη από τους οδηγούς `scbus` και `da`. Η καλύτερη απόδοση επιτυγχάνεται με θύρα σε κατάσταση λειτουργίας EPP 1.9.

```
#device         puc
```

Ενεργοποιήστε αυτή τη συσκευή αν έχετε μια "χαζή" σειριακή ή παράλληλη PCI κάρτα η οποία υποστηρίζεται από το πρόγραμμα οδήγησης puc(4) (glue driver).

```
# PCI Ethernet NICs.
device          de         # DEC/Intel DC21x4x (Tulip)
device          em         # Intel PRO/1000 adapter Gigabit Ethernet Card
```

```
device          ixgb       # Intel PRO/10GbE Ethernet Card
device          txp        # 3Com 3cR990 (Typhoon)
device          vx         # 3Com 3c590, 3c595 (Vortex)
```

Διάφορα προγράμματα οδήγησης για PCI κάρτες δικτύου. Μετατρέψτε σε σχόλιο ή αφαιρέστε τελείως όσες δεν υπάρχουν στο σύστημα σας.

```
# PCI Ethernet NICs that use the common MII bus controller code.
# NOTE: Be sure to keep the 'device miibus' line in order to use these NICs!
device          miibus     # MII bus support
```

Η υποστήριξη διαύλου MII απαιτείται για κάποιες κάρτες δικτύου Ethernet PCI 10/100, ειδικά για αυτές που χρησιμοποιούν πομποδέκτη συμβατό με MII ή έχουν διεπαφή ελέγχου που λειτουργεί παρόμοια με τον MII. Προσθέτοντας `device miibus` στο αρχείο ρύθμισης του πυρήνα, θα έχετε υποστήριξη για το γενικό API του miibus και για όλους τους οδηγούς PHY, συμπεριλαμβανομένου και ενός γενικού για PHYs που δεν υποστηρίζονται από κάποιο συγκεκριμένο οδηγό.

```
device          bce        # Broadcom BCM5706/BCM5708 Gigabit Ethernet
device          bfe        # Broadcom BCM440x 10/100 Ethernet
device          bge        # Broadcom BCM570xx Gigabit Ethernet
device          dc         # DEC/Intel 21143 and various workalikes
device          fxp        # Intel EtherExpress PRO/100B (82557, 82558)
device          lge        # Level 1 LXT1001 gigabit ethernet
device          msk        # Marvell/SysKonnect Yukon II Gigabit Ethernet
device          nge        # NatSemi DP83820 gigabit ethernet
device          nve        # nVidia nForce MCP on-board Ethernet Networking
device          pcn        # AMD Am79C97x PCI 10/100 (precedence over 'lnc')
device          re         # RealTek 8139C+/8169/8169S/8110S
device          rl         # RealTek 8129/8139
device          sf         # Adaptec AIC-6915 (Starfire)
device          sis        # Silicon Integrated Systems SiS 900/SiS 7016
device          sk         # SysKonnect SK-984x & SK-982x gigabit Ethernet
device          ste        # Sundance ST201 (D-Link DFE-550TX)
device          stge       # Sundance/Tamarack TC9021 gigabit Ethernet
device          ti         # Alteon Networks Tigon I/II gigabit Ethernet
device          tl         # Texas Instruments ThunderLAN
device          tx         # SMC EtherPower II (83c170 EPIC)
device          vge        # VIA VT612x gigabit ethernet
device          vr         # VIA Rhine, Rhine II
device          wb         # Winbond W89C840F
device          xl         # 3Com 3c90x (Boomerang, Cyclone)
```

Προγράμματα οδήγησης που χρησιμοποιούν τον κώδικα του διαύλου ελέγχου MII.

```
# ISA Ethernet NICs.  pccard NICs included.
device          cs         # Crystal Semiconductor CS89x0 NIC
# 'device ed' requires 'device miibus'
```

```
device          ed          # NE[12]000, SMC Ultra, 3c503, DS8390 cards
device          ex          # Intel EtherExpress Pro/10 and Pro/10+
device          ep          # Etherlink III based cards
device          fe          # Fujitsu MB8696x based cards
device          ie          # EtherExpress 8/16, 3C507, StarLAN 10 etc.
device          lnc         # NE2100, NE32-VL Lance Ethernet cards
device          sn          # SMC's 9000 series of Ethernet chips
device          xe          # Xircom pccard Ethernet

# ISA devices that use the old ISA shims
#device         le
```

Προγράμματα οδήγησης καρτών Ethernet τύπου ISA. Δείτε το αρχείο /usr/src/sys/i386/conf/NOTES για λεπτομέρειες σχετικά με το ποιες κάρτες υποστηρίζονται από ποιον οδηγό.

```
# Wireless NIC cards
device          wlan            # 802.11 support
```

Γενική υποστήριξη του 802.11. Η γραμμή αυτή απαιτείται για ασύρματη δικτύωση.

```
device          wlan_wep        # 802.11 WEP support
device          wlan_ccmp       # 802.11 CCMP support
device          wlan_tkip       # 802.11 TKIP support
```

Υποστήριξη κρυπτογράφησης για συσκευές 802.11. Οι γραμμές αυτές χρειάζονται αν σκοπεύετε να χρησιμοποιήσετε κρυπτογράφηση και πρωτόκολλα ασφαλείας 802.11i.

```
device          an          # Aironet 4500/4800 802.11 wireless NICs.
device          ath             # Atheros pci/cardbus NIC's
device          ath_hal         # Atheros HAL (Hardware Access Layer)
device          ath_rate_sample # SampleRate tx rate control for ath
device          awi         # BayStack 660 and others
device          ral         # Ralink Technology RT2500 wireless NICs.
device          wi          # WaveLAN/Intersil/Symbol 802.11 wireless NICs.
#device         wl          # Older non 802.11 Wavelan wireless NIC.
```

Υποστήριξη για διάφορες ασύρματες κάρτες.

```
# Pseudo devices
device   loop           # Network loopback
```

Πρόκειται για τη γενική συσκευή εσωτερικού δικτύου (loopback) του TCP/IP. Η σύνδεση μέσω telnet ή FTP στο `localhost` (γνωστό επίσης και ως `127.0.0.1`) πραγματοποιείται μέσω αυτής της συσκευής. Η ύπαρξη αυτής της συσκευής είναι *υποχρεωτική*.

```
device   random       # Entropy device
```

Κρυπτογραφικά ασφαλής γεννήτρια τυχαίων αριθμών.

```
device   ether        # Ethernet support
```

Η γραμμή `ether` απαιτείται μόνο αν έχετε κάρτα δικτύου Ethernet. Περιέχει γενικό κώδικα για το πρωτόκολλο Ethernet.

```
device   sl           # Kernel SLIP
```

Η γραμμή `sl` παρέχει υποστήριξη SLIP. Η υποστήριξη αυτή έχει σχεδόν ολοκληρωτικά ξεπεραστεί από το PPP, το οποίο είναι ευκολότερο στη ρύθμιση, υποστηρίζει καλύτερα τις συνδέσεις μέσω μόντεμ, και παρέχει καλύτερες δυνατότητες.

```
device   ppp          # Kernel PPP
```

Η γραμμή αυτή είναι για υποστήριξη PPP μέσω του πυρήνα για επιλογικές (dial-up) συνδέσεις. Υπάρχει επίσης μια έκδοση PPP η οποία υλοποιείται ως εφαρμογή χρήστη (userland), χρησιμοποιεί το `tun` και προσφέρει περισσότερη ευελιξία και λειτουργίες όπως κλήση κατά απαίτηση (demand dialing).

```
device   tun          # Packet tunnel.
```

Η συσκευή αυτή χρησιμοποιείται από το πρόγραμμα PPP χρήστη (userland). Δείτε το τμήμα PPP αυτού του βιβλίου για περισσότερες πληροφορίες.

```
device   pty          # Pseudo-ttys (telnet etc)
```

Πρόκειται για συσκευή "ψευδό-τερματικού" ή προσομοίωσης θύρας login. Χρησιμοποιείται για εισερχόμενες συνδέσεις `telnet` και `rlogin`, από το xterm, και από κάποιες άλλες εφαρμογές όπως το Emacs.

```
device   md           # Memory disks
```

Ψευτό-συσκευές δίσκου με χρήση μνήμης (ramdrives).

```
device   gif          # IPv6 and IPv4 tunneling
```

Η συσκευή αυτή υλοποιεί IPv6 σε IPv4 tunneling, IPv4 σε IPv6 tunneling, IPv4 σε IPv4 tunneling, και IPv6 σε IPv6 tunneling. Η συσκευή `gif` "αυτό-κλωνοποιείται", και δημιουργεί τα αντίστοιχα αρχεία

συσκευών όπως απαιτούνται.

```
device   faith         # IPv6-to-IPv4 relaying (translation)
```

Αυτή η ψεύδο-συσκευή συλλαμβάνει πακέτα που στέλνονται προς αυτήν και τα ανακατευθύνει προς το δαίμονα μετάφρασης του IPv4/IPv6.

```
# The `bpf' device enables the Berkeley Packet Filter.
# Be aware of the administrative consequences of enabling this!
# Note that 'bpf' is required for DHCP.
device   bpf           # Berkeley packet filter
```

Πρόκειται για το φίλτρο πακέτων Berkeley. Αυτή η ψεύδο-συσκευή επιτρέπει σε κάρτες δικτύου να λειτουργούν σε κατάσταση promiscuous (πλήρους ακρόασης), συλλαμβάνοντας με αυτό τον τρόπο κάθε πακέτο ενός δικτύου (π.χ. Ethernet). Τα πακέτα αυτά μπορεί να αποθηκεύονται στο δίσκο ή να εξετάζονται με τη βοήθεια του προγράμματος tcpdump(1).

Η συσκευή bpf(4) χρησιμοποιείται επίσης από το dhclient(8) για την ανάκτηση της διεύθυνσης IP της προεπιλεγμένης πύλης κ.ο.κ. Αν χρησιμοποιείτε DHCP, αφήστε αυτή την επιλογή ενεργοποιημένη.

```
# USB support
device          uhci          # UHCI PCI->USB interface
device          ohci          # OHCI PCI->USB interface
device          ehci          # EHCI PCI->USB interface (USB 2.0)
device          usb           # USB Bus (required)
#device         udbp          # USB Double Bulk Pipe devices
device          ugen          # Generic
device          uhid          # Human Interface Devices
device          ukbd          # Keyboard
device          ulpt          # Printer
device          umass         # Disks/Mass storage - Requires scbus and da
device          ums           # Mouse
device          ural          # Ralink Technology RT2500USB wireless NICs
device          urio          # Diamond Rio 500 MP3 player
device          uscanner      # Scanners
# USB Ethernet, requires mii
device          aue           # ADMtek USB Ethernet
device          axe           # ASIX Electronics USB Ethernet
device          cdce          # Generic USB over Ethernet
device          cue           # CATC USB Ethernet
device          kue           # Kawasaki LSI USB Ethernet
device          rue           # RealTek RTL8150 USB Ethernet
```

Υποστήριξη για διάφορες συσκευές USB.

```
# FireWire support
device          firewire      # FireWire bus code
device          sbp           # SCSI over FireWire (Requires scbus and da)
device          fwe           # Ethernet over FireWire (non-standard!)
```

Υποστήριξη για διάφορες συσκευές Firewire.

Για περισσότερες πληροφορίες και επιπλέον συσκευές που υποστηρίζονται από το FreeBSD, δείτε το αρχείο /usr/src/sys/i386/conf/NOTES.

15.6.1. Λειτουργία με Μεγάλη Ποσότητα Μνήμης (PAE)

Μηχανήματα με μεγάλη ποσότητα μνήμης, χρειάζονται πρόσβαση σε μνήμη που υπερβαίνει το όριο των 4 gigabytes των Εικονικών Διευθύνσεων Χρήστη+Πυρήνα (User+Kernel Virtual Address, KVA). Εξαιτίας αυτού του περιορισμού, η Intel πρόσθεσε υποστήριξη για 36bit φυσικών διευθύνσεων, από τον επεξεργαστή Pentium® Pro και μετά.

Η δυνατότητα Επέκτασης Φυσικών Διευθύνσεων, (Physical Address Extension, PAE) των Intel® Pentium® Pro και μεταγενέστερων CPU, επιτρέπει χρήση μνήμης ως 64 gigabytes. Το FreeBSD παρέχει υποστήριξη για τη δυνατότητα αυτή μέσω της ρύθμισης πυρήνα `PAE`, η οποία διατίθεται για όλες τις τρέχουσες σταθερές εκδόσεις του FreeBSD. Λόγω περιορισμών στην αρχιτεκτονική του συστήματος μνήμης της Intel, δεν γίνεται διάκριση για τη μνήμη που βρίσκεται πάνω ή κάτω από τα 4 gigabytes. Η μνήμη που εκχωρείται πάνω από τα 4 gigabytes, απλώς προστίθεται στο μέγεθος της διαθέσιμης μνήμης.

Για να ενεργοποιήσετε την υποστήριξη PAE στον πυρήνα, απλώς προσθέστε την ακόλουθη γραμμή στο αρχείο των ρυθμίσεων σας:

```
options         PAE
```

Η υποστήριξη PAE στο FreeBSD είναι διαθέσιμη μόνο για επεξεργαστές αρχιτεκτονικής Intel® IA-32. Θα πρέπει επίσης να σημειώσουμε ότι η υποστήριξη PAE στο FreeBSD δεν έχει δοκιμαστεί εκτεταμένα, και θα πρέπει να θεωρείται ποιότητας beta σε σχέση με τα άλλα σταθερά χαρακτηριστικά του FreeBSD.

Η υποστήριξη PAE στο FreeBSD υπόκειται σε κάποιους περιορισμούς:

- Μια διαδικασία δεν έχει πρόσβαση σε περισσότερα από 4 gigabytes χώρου VM.
- Οδηγοί συσκευών που δεν χρησιμοποιούν τη διεπαφή bus_dma(9) ίσως προκαλέσουν καταστροφή δεδομένων σε ένα PAE πυρήνα και για το λόγο αυτό δεν συνίσταται η χρήση τους. Στο FreeBSD παρέχεται ένα αρχείο ρυθμίσεων PAE στο οποίο έχουν εξαιρεθεί όλα τα προγράμματα οδήγησης που είναι γνωστό ότι δεν δουλεύουν σε πυρήνα τύπου PAE.
- Κάποιες μεταβλητές συστήματος (system tunables) εξακριβώνουν τη χρήση της μνήμης, βλέποντας το ποσό της διαθέσιμης φυσικής μνήμης. Αυτές οι μεταβλητές μπορεί να χρησιμοποιήσουν αδικαιολόγητα μεγάλη ποσότητα μνήμης, λόγω της φύσης του συστήματος PAE. Ένα τέτοιο παράδειγμα είναι η ρύθμιση sysctl `kern.maxvnodes` η οποία ελέγχει το μέγιστο

αριθμό vnodes που επιτρέπονται στον πυρήνα. Είναι σκόπιμο να ρυθμίσετε αυτή και άλλες παρόμοιες παραμέτρους σε λογικές τιμές.

- Ίσως χρειαστεί να ρυθμίσετε τις εικονικές διευθύνσεις του πυρήνα (KVA) ή να μειώσετε την ποσότητα κάποιου συγκεκριμένου πόρου που έχει μεγάλη χρήση (δείτε παραπάνω) για να αποφύγετε την εξάντληση του KVA. Μπορείτε να αυξήσετε το μέγεθος του KVA μέσω της επιλογής `KVA_PAGES`.

Για λόγους σταθερότητας και απόδοσης, σας συμβουλεύουμε να διαβάσετε τη σελίδα manual tuning(7). Επίσης η σελίδα pae(4) περιέχει ενημερωμένες πληροφορίες σχετικά με την υποστήριξη PAE στο FreeBSD.

15.7. Αν Κάτι Πάει Λάθος

Υπάρχουν τέσσερις κατηγορίες προβλημάτων που μπορούν να παρουσιαστούν όταν δημιουργείτε ένα προσαρμοσμένο πυρήνα:

Αποτυχία της εντολής `config`

Αν η εντολή config(8) αποτυγχάνει όταν της δίνετε την περιγραφή του πυρήνα σας, έχετε κατά πάσα πιθανότητα, κάνει κάποιο απλό λάθος. Ευτυχώς, η config(8) θα σας δείξει τον αριθμό γραμμής στον οποίο συνάντησε το πρόβλημα, και έτσι θα μπορέσετε εύκολα να το εντοπίσετε. Για παράδειγμα, αν δείτε:

```
config: line 17: syntax error
```

Βεβαιωθείτε ότι η λέξη-κλειδί στη γραμμή αυτή είναι σωστή, συγκρίνοντας τη με την αντίστοιχη στο αρχείο GENERIC ή σε άλλο αρχείο αναφοράς.

Αποτυχία της εντολής `make`

Αν αποτυγχάνει η εντολή `make`, συνήθως αυτό σημαίνει κάποιο λάθος στο αρχείο ρυθμίσεων το οποίο δεν είναι αρκετά σοβαρό για να το καταλάβει η config(8). Κοιτάξτε ξανά το αρχείο ρυθμίσεων σας και αν ακόμα δεν μπορείτε να εντοπίσετε το πρόβλημα, στείλτε το μαζί με το αρχείο με mail στην ηλεκτρονική λίστα γενικών ερωτήσεων του FreeBSD και θα εντοπιστεί πολύ γρήγορα.

Ο πυρήνας δεν εκκινεί:

Αν ο νέος σας πυρήνας δεν εκκινεί ή αποτυγχάνει να αναγνωρίσει τις συσκευές σας, μην πανικοβάλλεστε! Ευτυχώς, το FreeBSD έχει ένα εξαιρετικό μηχανισμό για να επανέλθετε από μη-συμβατούς πυρήνες. Απλώς επιλέξτε τον πυρήνα από τον οποίο θέλετε να ξεκινήσετε μέσω του συστήματος εκκίνησης (boot loader) του FreeBSD. Έχετε πρόσβαση σε αυτό, την ώρα που εμφανίζεται το μενού επιλογών εκκίνησης. Επιλέξτε "Escape to a loader prompt", αριθμός έξι. Στην προτροπή που εμφανίζεται, γράψτε την εντολή `boot kernel.old` ή το όνομα αρχείου ενός άλλου πυρήνα που ξεκινάει κανονικά. Όταν φτιάχνετε ένα νέο πυρήνα, είναι πάντα καλή ιδέα να έχετε πρόχειρο ένα πυρήνα που ξέρετε ότι δουλεύει.

Αφού εκκινήσετε με ένα καλό πυρήνα, μπορείτε να ελέγξετε το αρχείο ρυθμίσεων σας από την αρχή, και να προσπαθήσετε ξανά. Μια χρήσιμη πηγή πληροφοριών είναι το αρχείο /var/log/messages το οποίο μεταξύ άλλων καταγράφει όλα τα μηνύματα του πυρήνα από κάθε

επιτυχημένη εκκίνηση. Επίσης η εντολή dmesg(8) θα σας δείξει όλα τα μηνύματα του πυρήνα της τρέχουσας εκκίνησης.

Αν έχετε πρόβλημα στη δημιουργία πυρήνα, βεβαιωθείτε ότι έχετε κρατήσει ένα πυρήνα GENERIC, ή κάποιο άλλο που γνωρίζετε ότι λειτουργεί, χρησιμοποιώντας ένα διαφορετικό όνομα ώστε να μη διαγραφεί στην επόμενη μεταγλώττιση. Δεν μπορείτε να βασιστείτε στον πυρήνα kernel.old, γιατί κάθε φορά που εγκαθιστάτε νέο πυρήνα, το kernel.old αντικαθίσταται με τον τελευταίο εγκατεστημένο πυρήνα, ο οποίος μπορεί να μην λειτουργεί. Επίσης, όσο το δυνατόν πιο σύντομα, μετακινήστε τον πυρήνα που λειτουργεί στην σωστή θέση, /boot/kernel, διαφορετικά εντολές όπως η ps(1) ίσως να μη λειτουργούν σωστά. Για να το κάνετε αυτό, απλώς μετονομάστε τον κατάλογο που περιέχει τον καλό πυρήνα, π.χ:

```
# mv /boot/kernel /boot/kernel.bad
# mv /boot/kernel.good /boot/kernel
```

Ο νέος πυρήνας λειτουργεί, αλλά η ps(1) δεν λειτουργεί πλέον

Αν εγκαταστήσετε πυρήνα διαφορετικής έκδοσης από αυτόν με τον οποίο έχουν φτιαχτεί τα εργαλεία συστήματος, για παράδειγμα εάν βάλετε ένα πυρήνα της σειράς -CURRENT σε ένα σύστημα -RELEASE, πολλές από τις εντολές που σχετίζονται με την κατάσταση του συστήματος όπως ή ps(1) και η vmstat(8) δεν θα λειτουργούν πλέον. Θα πρέπει να μεταγλωττίσετε και να εγκαταστήσετε όλο το βασικό σύστημα (world) χρησιμοποιώντας ίδια έκδοση του πηγαίου κώδικα με αυτή του πυρήνα σας. Αυτός είναι και ένας λόγος για τον οποίο δεν είναι συνήθως καλή ιδέα να χρησιμοποιείτε διαφορετική έκδοση πυρήνα από το υπόλοιπο του λειτουργικού συστήματος.

Chapter 16. Εκτυπώσεις

16.1. Σύνοψη

Μπορείτε να χρησιμοποιήσετε το FreeBSD για να κάνετε εκτυπώσεις σε διάφορους τύπους εκτυπωτών, από τον παλαιότερο κρουστικό ως τον πιο σύγχρονο laser εκτυπωτή, καθώς και οποιασδήποτε άλλης τεχνολογίας ανάμεσα τους, και να δημιουργήσετε εκτυπώσεις υψηλής ποιότητας με τις εφαρμογές που εκτελείτε.

Το FreeBSD μπορεί επίσης να ρυθμιστεί ώστε να λειτουργεί ως εξυπηρετητής εκτυπώσεων δικτύου. Με αυτή τη δυνατότητα το FreeBSD μπορεί να λαμβάνει εργασίες εκτύπωσης από διάφορους άλλους υπολογιστές, συμπεριλαμβανομένων υπολογιστών FreeBSD, Windows® και Mac OS®. Το FreeBSD μπορεί να εξασφαλίζει ότι μόνο μια εργασία θα τυπώνεται κάθε χρονική στιγμή και μπορεί να τηρεί στατιστικά για τους χρήστες και τα μηχανήματα που θα κάνουν τις περισσότερες εκτυπώσεις, να παράγει σελίδες "banner" που να δείχνουν σε ποιόν ανήκει η κάθε εκτύπωση, και πολλά άλλα.

Αφού διαβάσετε αυτό το κεφάλαιο θα ξέρετε:

- Πως να ρυθμίσετε την ουρά εκτυπώσεων (print spooler) του FreeBSD.
- Πως να εγκαθιστάτε φίλτρα εκτύπωσης, να χειρίζεστε ειδικές εργασίες εκτύπωσης (π.χ. τη μετατροπή εισερχόμενων κειμένων σε μορφές εκτύπωσης που είναι κατανοητές από τους εκτυπωτές σας).
- Πως να ενεργοποιήσετε σελίδες τύπου κεφαλίδας ή banner στις εκτυπώσεις σας.
- Πως να εκτυπώνετε σε εκτυπωτές που είναι συνδεδεμένοι σε άλλους υπολογιστές.
- Πως να εκτυπώνετε σε εκτυπωτές που είναι συνδεδεμένοι απευθείας στο δίκτυο.
- Πως να ελέγχετε τους περιορισμούς εκτύπωσης, συμπεριλαμβανομένων των περιορισμών μεγέθους των εργασιών εκτύπωσης, και πως να παρεμποδίζετε την δυνατότητα εκτύπωσης σε συγκεκριμένους χρήστες.
- Πως να κρατήσετε στατιστικά για τον εκτυπωτή, και καταγραφή για τη χρήση του εκτυπωτή από κάθε χρήστη.
- Πως να αντιμετωπίσετε προβλήματα στις εκτυπώσεις.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να γνωρίζετε πως να ρυθμίσετε και να εγκαταστήσετε ένα νέο πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).

16.2. Εισαγωγή

Για να χρησιμοποιήσετε εκτυπωτές στο FreeBSD, θα χρειαστεί να ρυθμίσετε τη λειτουργία τους με το σύστημα παροχέτευσης (spooling) εκτυπωτών γραμμής του Berkeley, γνωστό επίσης και ως σύστημα παροχέτευσης LPD, ή απλά LPD. Αυτό είναι το προκαθορισμένο σύστημα ελέγχου εκτυπωτών στο FreeBSD. Το κεφάλαιο αυτό είναι μια εισαγωγή στο LPD και θα σας καθοδηγήσει στις ρυθμίσεις του.

Εάν σας είναι οικείο το LPD ή κάποιο άλλο σύστημα παροχέτευσης εκτυπωτών, τότε μπορείτε να μεταπηδήσετε στην ενότητα Βασική Εγκατάσταση.

Το LPD μπορεί να ελέγχει εξ' ολοκλήρου όλες τις λειτουργίες των εκτυπωτών ενός υπολογιστή. Είναι κυρίως υπεύθυνο για ένα πλήθος λειτουργιών:

- Ελέγχει την πρόσβαση σε απευθείας συνδεμένους εκτυπωτές και εκτυπωτές προσαρτημένους σε άλλους κόμβους στο δίκτυο.
- Επιτρέπει σε χρήστες να στέλνουν αρχεία προς εκτύπωση. Οι αποστολές αυτές είναι γνωστές ως *εργασίες (jobs)*.
- Διατηρεί *ουρά αναμονής (queue)* για κάθε εκτυπωτή, ώστε να προλαμβάνει την ταυτόχρονη πρόσβαση από πολλούς χρήστες.
- Μπορεί να εκτυπώνει *σελίδες κεφαλίδας* (γνωστές επίσης ως *banner* ή *σελίδες burst*) ώστε οι χρήστες να μπορούν εύκολα να ξεχωρίσουν τις εργασίες τους μέσα στην στοίβα εκτυπώσεων.
- Φροντίζει για την ορθότητα των παραμέτρων επικοινωνίας των εκτυπωτών που είναι συνδεδεμένοι σε σειριακές θύρες.
- Μπορεί μέσω του δικτύου να στείλει εργασίες σε σύστημα παροχέτευσης LPD διαφορετικού υπολογιστή.
- Μπορεί να εκτελέσει διάφορα φίλτρα για να προσαρμόσει εργασίες ώστε να είναι δυνατή η εκτύπωση τους σε εκτυπωτές που χρησιμοποιούν διαφορετικές γλώσσες ή έχουν διαφορετικές δυνατότητες.
- Μπορεί να κάνει καταμέτρηση χρήσης του εκτυπωτή.

Μέσω του αρχείου ρύθμισης (/etc/printcap), και με τη βοήθεια ειδικών προγραμμάτων φίλτρων, μπορείτε να ενεργοποιήσετε το σύστημα LPD να κάνει όλες ή κάποιες από τις παραπάνω εργασίες σε μια μεγάλη γκάμα συσκευών εκτύπωσης.

16.2.1. Γιατί θα πρέπει να χρησιμοποιείτε τον Spooler

Αν είστε ο μοναδικός χρήστης του συστήματος, θα αναρωτιέστε γιατί θα έπρεπε να ενδιαφερθείτε για τον spooler αφού δεν χρειάζεστε έλεγχο πρόσβασης, σελίδες κεφαλίδας, ή αναφορές εκτύπωσης. Αν και μπορείτε να ενεργοποιήσετε την άμεση πρόσβαση στον εκτυπωτή, είναι καλύτερα να χρησιμοποιείτε τον spooler για τους παρακάτω λόγους:

- το LPD εκτυπώνει τις εργασίες στο παρασκήνιο, δεν χρειάζεται να περιμένετε να αντιγραφούν τα δεδομένα στον εκτυπωτή.
- Το LPD μπορεί άνετα να εκτελεί μια εργασία εκτύπωσης διαμέσου φίλτρων και να προσθέτει κεφαλίδες ημερομηνίας/ώρας ή να μετατρέπει κάποιο ειδικό τύπο αρχείου (όπως ένα αρχείο TeX DVI) σε ένα τύπο κατανοητό από τον εκτυπωτή σας. Αυτές οι διαδικασίες δεν χρειάζεται να γίνονται χειροκίνητα.
- Πολλά από τα ελεύθερα και εμπορικά διαθέσιμα προγράμματα που παρέχουν διευκολύνσεις στην εκτύπωση, συνήθως επιζητούν να επικοινωνήσουν με τον spooler του συστήματος σας. Ρυθμίζοντας το σύστημα παροχέτευσης, θα μπορείτε ευκολότερα να υποστηρίζετε λογισμικό τρίτων, που μπορεί ήδη να έχετε ή που πρόκειται να εγκαταστήσετε στο μέλλον.

16.3. Βασική Εγκατάσταση

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών για τις σειριακές θύρες μετονομάστηκαν από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την τεκμηρίωση που ακολουθεί με βάση αυτές τις αλλαγές.

Για να χρησιμοποιήσετε εκτυπωτές με το σύστημα παροχέτευσης LPD, θα πρέπει να εγκαταστήσετε τόσο το hardware του εκτυπωτή σας όσο και το λογισμικό LPD. Αυτό το έγγραφο περιγράφει την εγκατάσταση σε δύο στάδια:

- Δείτε την ενότητα Βασικές Ρυθμίσεις Εκτυπωτών για να μάθετε πως γίνεται η σύνδεση εκτυπωτών, με ποιο τρόπο επικοινωνεί το LPD με τους εκτυπωτές, και πως να εκτυπώνετε απλά αρχεία κειμένου.
- Δείτε την ενότητα Ρυθμίσεις Εκτυπωτών για Προχωρημένους για να μάθετε πως να εκτυπώνετε αρχεία ειδικής μορφής διαφόρων τύπων, πως να εκτυπώνετε σελίδες κεφαλίδας, πως να εκτυπώνετε σε ένα δίκτυο, πως να ελέγχετε την πρόσβαση στους εκτυπωτές, και πως να χρησιμοποιείτε την καταγραφή εκτυπώσεων.

16.3.1. Βασικές Ρυθμίσεις Εκτυπωτών

Αυτή η ενότητα περιγράφει πως να ρυθμίσετε το hardware του εκτυπωτή και το λογισμικό LPD. Παρέχει βασικές γνώσεις για τα εξής θέματα:

- Η Ενότητα Ρυθμίσεις Hardware υποδεικνύει πως να συνδέσετε τον εκτυπωτή σε μια θύρα του υπολογιστή σας.
- Η Ενότητα Ρυθμίσεις Λογισμικού υποδεικνύει πως να εγκαταστήσετε το αρχείο ρύθμισης του συστήματος παροχέτευσης LPD: το αρχείο /etc/printcap.

Αν προσπαθείτε να εγκαταστήσετε έναν εκτυπωτή που δέχεται δεδομένα μέσω πρωτοκόλλου δικτύου και όχι μέσω διασύνδεσης τοπικής θύρας, τότε δείτε την ενότητα Εκτυπωτές Με Συνδέσεις Δικτύου.

Αν και αυτή η ενότητα ονομάζεται "Βασικές Ρυθμίσεις Εκτυπωτών", στην πραγματικότητα είναι αρκετά περίπλοκη. Το δυσκολότερο στάδιο στην εγκατάσταση είναι η επιτυχής λειτουργία στην επικοινωνία του εκτυπωτή με τον υπολογιστή σας και το σύστημα παροχέτευσης LPD. Οι επιλογές για προχωρημένους, όπως οι σελίδες κεφαλίδας και αναφοράς είναι σχετικά εύκολες να επιτευχθούν, μετά την επιτυχή ρύθμιση της βασικής λειτουργίας εκτύπωσης.

16.3.1.1. Ρυθμίσεις Hardware

Αυτή η ενότητα εξηγεί τους διάφορους τρόπους σύνδεσης του εκτυπωτή με τον υπολογιστή σας. Περιγράφει τους διάφορους τύπους θυρών και καλωδίων, και τις ρυθμίσεις που πρέπει να κάνετε στον πυρήνα για να ενεργοποιήσετε την επικοινωνία μεταξύ FreeBSD και εκτυπωτή.

Αν ήδη έχετε καταφέρει να συνδέσετε τον εκτυπωτή σας και έχετε εκτυπώσει επιτυχώς σε άλλο λειτουργικό σύστημα, τότε μπορείτε να μεταβείτε κατευθείαν στην ενότητα Ρυθμίσεις Λογισμικού.

16.3.1.1.1. Θύρες και Καλώδια

Οι εκτυπωτές που διατίθενται σήμερα για χρήση με Η/Υ παρέχονται με μία ή περισσότερες εκ των ακολούθων τριών διασυνδέσεων:

- Οι *Σειριακές* διασυνδέσεις, γνωστές και ως RS-232 ή θύρες COM, χρησιμοποιούν την σειριακή θύρα του υπολογιστή σας για να στείλουν δεδομένα στον εκτυπωτή. Οι σειριακές διασυνδέσεις είναι συνήθεις στην βιομηχανία κατασκευής Η/Υ και τα καλώδια είναι εκτενώς διαδεδομένα και επίσης εύκολα να κατασκευαστούν. Οι σειριακές διασυνδέσεις μερικές φορές χρειάζονται ειδικά καλώδια και μπορεί να σας ζητηθούν πολύπλοκες επικοινωνιακές ρυθμίσεις. Οι περισσότερες σειριακές θύρες των Η/Υ έχουν μέγιστη ταχύτητα μετάδοσης 115200 bps, κάνοντας δύσκολη την εργασία εκτύπωσης γραφικών μεγάλων διαστάσεων.
- Οι *Παράλληλες* διασυνδέσεις χρησιμοποιούν την παράλληλη θύρα του υπολογιστή σας για να στέλνουν δεδομένα στον εκτυπωτή. Οι παράλληλες διασυνδέσεις είναι διαδεδομένες στο εμπόριο και είναι γρηγορότερες από τις σειριακές RS-232. Τα καλώδια διατίθενται έτοιμα, αλλά είναι δυσκολότερο να κατασκευαστούν χειρωνακτικά. Με τις παράλληλες διασυνδέσεις δεν προβλέπονται επιλογές ρύθμισης επικοινωνίας, κάνοντας την ρύθμιση τους εξαιρετικά απλή.

  Οι παράλληλες διασυνδέσεις είναι γνωστές και ως διασυνδέσεις "Centronics", ονομασία προερχόμενη από τον τύπο του ακροδέκτη του εκτυπωτή.

- Οι διασυνδέσεις USB, συντομογραφία από το Universal Serial Bus, δουλεύουν σε ακόμη μεγαλύτερες ταχύτητες από την παράλληλη και την RS-232 σειριακή διασύνδεση. Τα καλώδια τους είναι απλά και φτηνά. Η USB είναι ανώτερη από την Σειριακή RS-232 και από την Παράλληλη στην εκτύπωση, αλλά δυστυχώς δεν υποστηρίζεται καλά από τα συστήματα UNIX®. Ένας τρόπος για να αποφύγετε αυτό το πρόβλημα είναι να αγοράσετε εκτυπωτή που φέρει διασύνδεση USB και Παράλληλη, όπως συμβαίνει με πολλούς εκτυπωτές.

Γενικά, οι Παράλληλες διασυνδέσεις προσφέρουν συνήθως μίας κατεύθυνσης επικοινωνία (από τον υπολογιστή στον εκτυπωτή) ενώ η σειριακή και η USB δίνουν αμφίδρομη. Στο FreeBSD οι πιο πρόσφατες παράλληλες θύρες (EPP και ECP) καταφέρνουν αμφίδρομη επικοινωνία με τους εκτυπωτές, όταν χρησιμοποιούνται καλώδια που συμμορφώνονται με το πρότυπο IEEE-1284.

Η αμφίδρομη επικοινωνία με εκτυπωτές διαμέσου παράλληλης θύρας μπορεί να επιτευχθεί γενικά με δύο τρόπους. Ο πρώτος τρόπος χρησιμοποιεί ένα προσαρμοσμένο πρόγραμμα οδήγησης εκτυπωτή, ώστε να μπορεί το FreeBSD να συνομιλεί στην γλώσσα του εκτυπωτή. Αυτό είναι σύνηθες με εκτυπωτές inkjet και μπορεί επίσης να χρησιμοποιηθεί για αναφορές διαθέσιμης ποσότητας μελανιού και για άλλες πληροφορίες λειτουργίας. Η δεύτερη μέθοδος χρησιμοποιείται όταν ο εκτυπωτής έχει δυνατότητα υποστήριξης PostScript®.

Οι εργασίες PostScript® είναι στην πραγματικότητα προγράμματα που αποστέλλονται στον εκτυπωτή, δεν είναι απαραίτητο να παράγουν εκτυπώσεις, ενώ μπορούν να επιστρέψουν το αποτέλεσμα τους απευθείας στον υπολογιστή. Το PostScript® χρησιμοποιεί αμφίδρομη επικοινωνία για να ενημερώσει τον υπολογιστή για τυχόν προβλήματα, όπως σφάλματα στο πρόγραμμα PostScript® ή μπλοκάρισμα τροφοδοσίας χαρτιού. Οι χρήστες σας, θα σας είναι ευγνώμονες για αυτές τις πληροφορίες. Επιπλέον, ο καλύτερος τρόπος για να κάνετε σωστή καταμέτρηση με ένα αμφίδρομο εκτυπωτή PostScript® είναι: να ρωτήσετε τον εκτυπωτή για την συνολική καταμέτρηση των σελίδων του (πόσες σελίδες εκτύπωσε σε όλη τη διάρκεια ζωής του), μετά να αποστείλετε την εργασία του χρήστη, και έπειτα να ξαναρωτήσετε για την καταμέτρηση των σελίδων του. Αφαιρέστε

τις δύο τιμές και θα γνωρίζετε πόσες σελίδες να χρεώσετε στον χρήστη.

16.3.1.1.2. Παράλληλες Θύρες

Για να συνδέσετε έναν εκτυπωτή σε παράλληλη θύρα, συνδέστε το καλώδιο Centronics μεταξύ εκτυπωτή και υπολογιστή. Οι οδηγίες που συνοδεύουν τον εκτυπωτή και τον υπολογιστή θα σας καθοδηγήσουν να ολοκληρώσετε την σύνδεση.

Θυμηθείτε ποια παράλληλη θύρα χρησιμοποιείτε στον υπολογιστή. Η πρώτη παράλληλη θύρα στο FreeBSD είναι η ppc0, η δεύτερη είναι η ppc1, και ούτω καθεξής. Το όνομα συσκευής του εκτυπωτή χρησιμοποιεί την ίδια αρίθμηση: /dev/lpt0 για τον εκτυπωτή στην πρώτη παράλληλη θύρα κ.τ.λ.

16.3.1.1.3. Σειριακές Θύρες

Για να συνδέσετε έναν εκτυπωτή χρησιμοποιώντας σειριακή διασύνδεση, συνδέστε το κατάλληλο σειριακό καλώδιο μεταξύ εκτυπωτή και υπολογιστή. Οι οδηγίες που συνοδεύουν τον εκτυπωτή και τον υπολογιστή σας, θα σας καθοδηγήσουν να ολοκληρώσετε την σύνδεση.

Αν δεν είστε σίγουροι ποιο είναι το "κατάλληλο σειριακό καλώδιο", μπορείτε να δοκιμάσετε μία από τις ακόλουθες εναλλακτικές:

- Ένα καλώδιο *modem* ενώνει κάθε pin του ακροδέκτη από τη μια πλευρά του καλωδίου κατευθείαν με το αντίστοιχο pin του ακροδέκτη στο άλλο άκρο. Αυτός ο τύπος καλωδίου είναι γνωστός και ως καλώδιο "DTE-to-DCE".
- Ένα καλώδιο *null-modem* ενώνει κατευθείαν μερικά pins, ανταλλάσσει μερικά άλλα (για παράδειγμα, τα pins αποστολής και λήψης), ενώ βραχυκυκλώνει μερικά άλλα, εσωτερικά, στο προστατευτικό κάλυμμα κάθε ακροδέκτη. Αυτός ο τύπος καλωδίου είναι γνωστός και ως καλώδιο "DTE-to-DTE".
- Ένα καλώδιο *σειριακού εκτυπωτή*, που απαιτείται από κάποιους λιγότερο συνηθισμένους εκτυπωτές, είναι σαν το καλώδιο null-modem, αλλά στέλνει ισοδύναμα σήματα και στα δύο άκρα αντί να τα βραχυκυκλώνει εσωτερικά.

Θα πρέπει επίσης να ρυθμίσετε τις παραμέτρους επικοινωνίας του εκτυπωτή, συνήθως από τον μπροστινό πίνακα ελέγχου ή από τους DIP διακόπτες του. Επιλέξτε την μέγιστη τιμή `bps` (bits per second = bits ανά δευτερόλεπτο, αναφέρεται και ως *ρυθμός baud*) που υποστηρίζουν ο υπολογιστής και ο εκτυπωτής σας. Επιλέξτε 7 ή 8 data bits, none, even, ή odd parity, και 1 ή 2 stop bits. Επίσης επιλέξτε ένα πρωτόκολλο ελέγχου ροής: είτε none, ή XON/XOFF (αναφέρεται και ως έλεγχος ροής "in-band" ή "software"). Να θυμάστε αυτές τις ρυθμίσεις, για το στάδιο ρύθμισης λογισμικού που ακολουθεί.

16.3.1.2. Ρυθμίσεις Λογισμικού

Αυτή η ενότητα περιγράφει τις αναγκαίες ρυθμίσεις που πρέπει να γίνουν στο λογισμικό για να μπορείτε να εκτυπώνετε με το σύστημα παροχέτευσης εκτυπωτών LPD στο FreeBSD.

Μια γενική άποψη των ενεργειών που πρέπει να ακολουθήσετε είναι:

1. Ρυθμίστε τον πυρήνα σας, αν είναι αναγκαίο, για την θύρα που χρησιμοποιείτε για τον εκτυπωτή σας. Οι απαραίτητες ρυθμίσεις περιγράφονται στην ενότητα Ρυθμίσεις Πυρήνα.

2. Ρυθμίστε την κατάσταση επικοινωνίας για την παράλληλη θύρα, αν πρόκειται να την χρησιμοποιήσετε. Η ενότητα Ρυθμίσεις Κατάστασης Επικοινωνίας για την Παράλληλη Θύρα περιέχει λεπτομέρειες.
3. Ελέγξτε αν το λειτουργικό σύστημα μπορεί να στείλει δεδομένα στον εκτυπωτή. Η ενότητα Έλεγχος Επικοινωνίας του Εκτυπωτή παρέχει μερικές συμβουλές για το πως θα μπορούσε να γίνει ο έλεγχος.
4. Ρυθμίστε το LPD για τον εκτυπωτή σας, τροποποιώντας το αρχείο /etc/printcap. Θα βρείτε οδηγίες για αυτές τις ρυθμίσεις σε επόμενο τμήμα αυτού του κεφαλαίου.

16.3.1.2.1. Ρυθμίσεις Πυρήνα

Ο πυρήνας του λειτουργικού συστήματος έχει μεταγλωττιστεί έτσι ώστε να δουλεύει με ένα συγκεκριμένο σύνολο συσκευών. Η σειριακή και η παράλληλη διασύνδεση του εκτυπωτή είναι μέρος αυτού του συνόλου. Επομένως, ίσως να είναι αναγκαίο να προσθέσετε υποστήριξη για κάποια πρόσθετη σειριακή ή παράλληλη θύρα, αν δεν είναι ήδη ρυθμισμένη στον πυρήνα σας.

Για να ελέγξετε αν ο πυρήνας σας μπορεί να υποστηρίξει μια σειριακή διασύνδεση, πληκτρολογήστε:

```
# grep sioN /var/run/dmesg.boot
```

Όπου *N* είναι ο αριθμός της σειριακής θύρας, ξεκινώντας από το μηδέν. Αν δείτε στην έξοδο του τερματικού σας κάτι παρόμοιο με:

```
sio2 at port 0x3e8-0x3ef irq 5 on isa
sio2: type 16550A
```

τότε ο πυρήνας υποστηρίζει αυτή τη θύρα.

Για να ελέγξετε αν ο πυρήνας σας υποστηρίζει παράλληλες διασυνδέσεις, πληκτρολογήστε:

```
# grep ppcN /var/run/dmesg.boot
```

Όπου *N* είναι ο αριθμός της παράλληλης θύρας, ξεκινώντας από το μηδέν. Αν δείτε στην έξοδο του τερματικού σας κάτι παρόμοιο με:

```
ppc0: <Parallel port> at port 0x378-0x37f irq 7 on isa0
ppc0: SMC-like chipset (ECP/EPP/PS2/NIBBLE) in COMPATIBLE mode
ppc0: FIFO with 16/16/8 bytes threshold
```

τότε ο πυρήνας υποστηρίζει αυτή τη θύρα.

Για να μπορεί το λειτουργικό σύστημα να αναγνωρίζει και να χρησιμοποιεί την θύρα (παράλληλη ή σειριακή) για τον εκτυπωτή σας, ίσως χρειαστεί να επαναπροσαρμόσετε τον πυρήνα σας.

Για την υποστήριξη σειριακής θύρας, δείτε την ενότητα στις ρυθμίσεις του πυρήνα. Για την υποστήριξη παράλληλης θύρας, δείτε την ίδια ενότητα *και* την ενότητα που ακολουθεί.

16.3.1.3. Ρυθμίσεις Κατάστασης Επικοινωνίας για την Παράλληλη Θύρα

Όταν χρησιμοποιείτε την παράλληλη διασύνδεση, μπορείτε να επιλέξετε αν η επικοινωνία του FreeBSD με τον εκτυπωτή θα είναι τύπου interrupt-driven ή polled. Ο γενικός οδηγός συσκευής του εκτυπωτή (lpt(4)) στο FreeBSD χρησιμοποιεί το σύστημα ppbus(4), το οποίο ελέγχει την θύρα του chipset με τον οδηγό ppc(4).

- Η μέθοδος *interrupt-driven* είναι προεπιλεγμένη στον πυρήνα GENERIC. Με αυτή τη μέθοδο, το λειτουργικό σύστημα χρησιμοποιεί ένα σήμα IRQ για να προσδιορίσει αν ο εκτυπωτής είναι έτοιμος για δεδομένα.
- Η μέθοδος *polled* οδηγεί το λειτουργικό σύστημα να ζητά κατά επανάληψη από τον εκτυπωτή αν είναι έτοιμος για πρόσθετα δεδομένα. Όταν απαντήσει θετικά, ο πυρήνας στέλνει πρόσθετα δεδομένα.

Η μέθοδος interrupt-driven είναι συνήθως κάπως γρηγορότερη αλλά χρησιμοποιεί μια πολύτιμη γραμμή IRQ. Έχει παρατηρηθεί πως κάποιοι σύγχρονοι εκτυπωτές HP δε δουλεύουν σωστά σε κατάσταση interrupt, πιθανώς λόγω κάποιων (όχι απόλυτα εξακριβωμένων) προβλημάτων συγχρονισμού. Αυτοί οι εκτυπωτές χρειάζονται την μέθοδο polled. Θα πρέπει να χρησιμοποιείτε την αποτελεσματικότερη κατάσταση λειτουργίας. Κάποιοι εκτυπωτές δουλεύουν και στις δυο καταστάσεις, αλλά είναι οδυνηρά αργοί στην κατάσταση λειτουργίας interrupt.

Μπορείτε να ρυθμίσετε την κατάσταση επικοινωνίας με δύο τρόπους: ρυθμίζοντας τον πυρήνα ή χρησιμοποιώντας το πρόγραμμα lptcontrol(8).

Για να θέσετε την κατάσταση επικοινωνίας ρυθμίζοντας τον πυρήνα:

1. Επεξεργαστείτε το αρχείο ρύθμισης του πυρήνα. Δείτε την καταχώριση `ppc0`. Αν εγκαθιστάτε την δεύτερη παράλληλη θύρα, τότε χρησιμοποιείστε `ppc1`. Για την τρίτη θύρα `ppc2` και ούτω καθεξής.

   - Αν επιθυμείτε κατάσταση λειτουργίας interrupt-driven, επεξεργαστείτε την ακόλουθη γραμμή:

     ```
     hint.ppc.0.irq="N"
     ```

     στο αρχείο /boot/device.hints και αντικαταστήστε το *N* με τον σωστό αριθμό IRQ. Το αρχείο ρύθμισης του πυρήνα πρέπει επίσης να περιέχει τον οδηγό ppc(4):

     ```
     device ppc
     ```

   - Αν επιθυμείτε κατάσταση λειτουργίας polled, διαγράψτε από το αρχείο /boot/device.hints, την ακόλουθη γραμμή:

     ```
     hint.ppc.0.irq="N"
     ```

Σε μερικές περιπτώσεις, το παραπάνω δεν είναι αρκετό για να θέσετε την θύρα σε κατάσταση polled. Τις περισσότερες φορές το πρόβλημα προέρχεται από τον οδηγό acpi(4), ο οποίος έχει την ευχέρεια να εξετάζει και να προσαρτά συσκευές, και επομένως, να ελέγχει τον τρόπο πρόσβασης στην θύρα του εκτυπωτή. Θα πρέπει να ελέγξετε τις ρυθμίσεις του acpi(4) για να διορθώσετε αυτό το πρόβλημα.

2. Αποθηκεύστε το αρχείο. Ρυθμίστε, μεταγλωττίστε, και εγκαταστήστε τον πυρήνα, και έπειτα κάντε επανεκκίνηση. Για περισσότερες λεπτομέρειες, δείτε τις ρυθμίσεις του πυρήνα.

Για να θέσετε την κατάσταση επικοινωνίας με το lptcontrol(8):

1. Πληκτρολογήστε:

```
# lptcontrol -i -d /dev/lptN
```

για να θέσετε την κατάσταση λειτουργίας interrupt-driven για το `lptN`.

2. Πληκτρολογήστε:

```
# lptcontrol -p -d /dev/lptN
```

για να θέσετε την κατάσταση λειτουργίας polled για το `lptN`.

Θα μπορούσατε να καταχωρίσετε αυτές τις εντολές στο δικό σας αρχείο /etc/rc.local. Έτσι θα εκτελούνται αυτόματα κατά την εκκίνηση του συστήματος σας. Για περισσότερες πληροφορίες δείτε το lptcontrol(8).

16.3.1.4. Έλεγχος Επικοινωνίας του Εκτυπωτή

Πριν συνεχίσουμε να ρυθμίζουμε το σύστημα παροχέτευσης, θα πρέπει να βεβαιωθείτε ότι το λειτουργικό σύστημα μπορεί να στείλει επιτυχώς δεδομένα στον εκτυπωτή σας. Είναι ευκολότερο να κάνουμε ξεχωριστά την αποσφαλμάτωση επικοινωνίας του εκτυπωτή και την αποσφαλμάτωση του συστήματος παροχέτευσης.

Θα ελέγξουμε τον εκτυπωτή στέλνοντας μερικά δεδομένα κειμένου. Για εκείνους τους εκτυπωτές που μπορούν να εκτυπώνουν άμεσα τους χαρακτήρες που έχουν αποσταλεί, το πρόγραμμα lptest(1) είναι τέλειο: Παράγει όλους τους εκτυπώσιμους χαρακτήρες (96) ASCII σε 96 γραμμές.

Για εκτυπωτές PostScript® (ή που βασίζονται σε άλλη γλώσσα), θα χρειαστεί να κάνουμε ένα πιο πολύπλοκο τεστ. Ένα μικρό πρόγραμμα PostScript®, όπως αυτό που ακολουθεί, επαρκεί:

```
%!PS
100 100 moveto 300 300 lineto stroke
310 310 moveto /Helvetica findfont 12 scalefont setfont
(Is this thing working?) show
showpage
```

Ο παραπάνω κώδικας PostScript® μπορεί να τοποθετηθεί σε ένα αρχείο και να χρησιμοποιηθεί όπως υποδεικνύουν τα παραδείγματα στις ακόλουθες ενότητες.

Όταν αυτό το έγγραφο αναφέρεται σε μια γλώσσα εκτυπωτή, εννοείται μια γλώσσα όπως η PostScript®, αλλά όχι η PCL της Hewlett Packard - η PCL είναι μια γλώσσα ευρείας λειτουργικότητας η οποία επιτρέπει την ανάμιξη απλού κειμένου με ακολουθίες διαφυγής. Η PostScript® δεν μπορεί να εκτυπώσει άμεσα απλό κείμενο, και αυτός είναι ακριβώς ο τύπος της γλώσσας εκτυπωτή που θα πρέπει να διευθετήσουμε κατάλληλα.

16.3.1.4.1. Έλεγχος Παράλληλου Εκτυπωτή

Αυτή η ενότητα υποδεικνύει πως να ελέγξετε αν το FreeBSD μπορεί να επικοινωνήσει με έναν εκτυπωτή συνδεδεμένο σε παράλληλη θύρα.

Για να ελέγξετε έναν εκτυπωτή σε παράλληλη θύρα:

1. Γίνετε `root` με su(1).
2. Στείλτε δεδομένα στον εκτυπωτή.
   - Αν ο εκτυπωτής μπορεί να εκτυπώσει απλό κείμενο, τότε χρησιμοποιήστε το lptest(1). Πληκτρολογήστε:

     ```
     # lptest > /dev/lptN
     ```

     Όπου *N* είναι ο αριθμός της παράλληλης θύρας, ξεκινώντας από το μηδέν.
   - Εάν ο εκτυπωτής καταλαβαίνει PostScript® ή κάποια άλλη γλώσσα εκτυπωτών, τότε στείλτε ένα μικρό πρόγραμμα στον εκτυπωτή. Πληκτρολογήστε:

     ```
     # cat > /dev/lptN
     ```

     Έπειτα πληκτρολογήστε το πρόγραμμα μία προς μία γραμμή, *προσεκτικά*, γιατί δεν μπορείτε να επεξεργαστείτε μια γραμμή αφότου έχετε πιέσει το πλήκτρο `RETURN` ή `ENTER`. Αφού τελειώσετε με την καταχώριση του προγράμματος, πιέστε `CONTROL+D`, ή άλλο πλήκτρο τερματισμού αρχείου.

     Εναλλακτικά, μπορείτε να τοποθετήσετε το πρόγραμμα σε ένα αρχείο και να πληκτρολογήσετε:

     ```
     # cat file > /dev/lptN
     ```

   Όπου *file* είναι το όνομα του αρχείου που περιέχει το πρόγραμμα που θέλετε να στείλετε στον εκτυπωτή.

Θα δείτε κάτι να εκτυπώνεται. Μην ανησυχείτε αν το κείμενο δεν φαίνεται σωστό. Θα το διορθώσουμε αργότερα.

16.3.1.4.2. Έλεγχος Σειριακού Εκτυπωτή

Αυτή η ενότητα υποδεικνύει πως να ελέγξετε αν το FreeBSD μπορεί να επικοινωνήσει με έναν εκτυπωτή συνδεδεμένο σε σειριακή θύρα.

Για να ελέγξετε έναν εκτυπωτή σε σειριακή θύρα:

1. Γίνετε `root` με su(1).
2. Επεξεργαστείτε το αρχείο /etc/remote. Προσθέστε την ακόλουθη καταχώριση:

   ```
   printer:dv=/dev/port:br#bps-rate:pa=parity
   ```

   Όπου *port* είναι η καταχώριση συσκευής για την σειριακή πόρτα (`ttyu0`, `ttyu1`, κτλ.), *bps-rate* είναι η ταχύτητα bits-per-second επικοινωνίας με τον εκτυπωτή, και *parity* η ισοτιμία που απαιτείται από τον εκτυπωτή (`even`, `odd`, `none`, ή `zero`).

   Παρακάτω φαίνεται ένα υπόδειγμα καταχώρισης, για έναν εκτυπωτή συνδεδεμένο μέσω σειριακής γραμμής στην τρίτη σειριακή θύρα με ταχύτητα 19200 bps και χωρίς parity:

   ```
   printer:dv=/dev/ttyu2:br#19200:pa=none
   ```

3. Συνδεθείτε στον εκτυπωτή με tip(1). Πληκτρολογήστε:

   ```
   # tip printer
   ```

   Αν αυτό το στάδιο δεν δουλεύει, επεξεργαστείτε πάλι το αρχείο /etc/remote και προσπαθήστε το χρησιμοποιώντας /dev/cuaaN αντί για /dev/ttyuN.

4. Στείλτε δεδομένα στον εκτυπωτή.

   - Αν ο εκτυπωτής μπορεί να εκτυπώσει απλό κείμενο, χρησιμοποιήστε lptest(1). Γράψτε:

     ```
     % $lptest
     ```

   - Εάν ο εκτυπωτής καταλαβαίνει PostScript® ή κάποια άλλη γλώσσα εκτυπωτών, τότε στείλτε ένα μικρό πρόγραμμα στον εκτυπωτή. Πληκτρολογήστε το πρόγραμμα, μία προς μία γραμμή, *πολύ προσεκτικά*, καθώς ο εκτυπωτής μπορεί να ερμηνεύει διαφορετικά την χρήση χαρακτήρων όπως το backspace ή άλλων που παράγονται από διάφορα πλήκτρα επεξεργασίας. Μπορεί επίσης να χρειαστεί να πληκτρολογήσετε κάποιο ειδικό πλήκτρο τερματισμού αρχείου για τον εκτυπωτή ώστε να γνωρίζει πότε ολοκληρώνεται το πρόγραμμα. Για εκτυπωτές PostScript®, πιέστε `CONTROL+D`.

     Εναλλακτικά, μπορείτε να τοποθετήσετε το πρόγραμμα σε ένα αρχείο και να πληκτρολογήσετε:

```
% >file
```

Όπου *file* είναι το όνομα του αρχείου που περιέχει το πρόγραμμα. Αφού το tip(1) στείλει το αρχείο, πιέστε το κατάλληλο πλήκτρο τερματισμού αρχείου, αν απαιτείται.

Θα δείτε κάτι να εκτυπώνεται. Μην ανησυχείτε αν το κείμενο δεν φαίνεται σωστό. Θα το διορθώσουμε αργότερα.

16.3.1.5. Ενεργοποίηση του Spooler: το Αρχείο /etc/printcap

Σε αυτό το σημείο, ο εκτυπωτής σας θα πρέπει να είναι συνδεμένος, ο πυρήνας σας ρυθμισμένος να επικοινωνεί μαζί του (αν χρειάζεται), και έχετε πετύχει να στείλετε κάποια δοκιμαστικά δεδομένα στον εκτυπωτή. Είστε τώρα έτοιμοι να ρυθμίσετε το LPD για να ελέγχετε την πρόσβαση στον εκτυπωτή σας.

Μπορείτε να ρυθμίσετε το LPD με επεξεργασία του αρχείου /etc/printcap. Το σύστημα παροχέτευσης LPD διαβάζει αυτό το αρχείο κάθε φορά που χρησιμοποιείται ο spooler, επομένως πιθανές αναβαθμίσεις του μπαίνουν άμεσα σε εφαρμογή.

Είναι εύκολο να κατανοήσετε την μορφή του αρχείου printcap(5). Χρησιμοποιήστε τον κειμενογράφο που προτιμάτε για να κάνετε αλλαγές στο /etc/printcap. Η μορφή του είναι παρόμοια με άλλα αρχεία περιγραφής δυνατοτήτων, όπως τα /usr/shared/misc/termcap και /etc/remote. Δείτε την cgetent(3) για λεπτομερείς πληροφορίες σχετικά με την μορφή του αρχείου.

Η πιο απλή ρύθμιση του spooler αποτελείται από τα ακόλουθα βήματα:

1. Επιλέξτε ένα όνομα (και λίγα βολικά παρωνύμια) για τον εκτυπωτή, και τοποθετήστε τα στο αρχείο /etc/printcap. Δείτε την ενότητα Ονοματοδότηση Εκτυπωτή για περισσότερες πληροφορίες σχετικά με την ονομασία των εκτυπωτών.
2. Απενεργοποιήστε τις σελίδες κεφαλίδας (είναι ενεργές από προεπιλογή) εισάγοντας την ικανότητα `sh`. Για περισσότερες πληροφορίες δείτε την ενότητα Παρεμπόδιση Σελίδων Κεφαλίδας.
3. Δημιουργήστε ένα κατάλογο παροχέτευσης, και καθορίστε την τοποθεσία του με την ικανότητα `sd`. Για περισσότερες πληροφορίες δείτε την ενότητα Δημιουργία Καταλόγου Παροχέτευσης.
4. Καθορίστε την κατάλληλη καταχώριση /dev για τον εκτυπωτή, και σημειώστε τη στο /etc/printcap με την ικανότητα `lp`. Για περισσότερες πληροφορίες, δείτε την ενότητα Αναγνώριση της Συσκευής Εκτύπωσης. Επίσης, αν ο εκτυπωτής είναι σε σειριακή θύρα, εγκαταστήστε τις παραμέτρους επικοινωνίας με την ικανότητα `ms#` η οποία αναλύεται στην ενότητα Ρυθμίσεις Παραμέτρων Επικοινωνίας του Spooler.
5. Εγκαταστήστε φίλτρα εισόδου απλού κειμένου. Δείτε την ενότητα Εγκατάσταση Φίλτρου Κειμένου για περισσότερες πληροφορίες.
6. Ελέγξτε την εγκατάσταση εκτυπώνοντας οτιδήποτε με την εντολή lpr(1). Περισσότερες πληροφορίες είναι διαθέσιμες στις ενότητες Δοκιμή του Spooler και Εντοπισμός Βλαβών.

Εκτυπωτές που βασίζονται σε γλώσσες εκτύπωσης, όπως οι εκτυπωτές PostScript®, δεν μπορούν να εκτυπώσουν άμεσα απλό κείμενο. Ο απλός τρόπος ρύθμισης που δείξαμε παραπάνω και που θα περιγράψουμε εκτενέστερα στις επόμενες ενότητες,

> προϋποθέτει πως αν ρυθμίζετε έναν τέτοιο εκτυπωτή θα μπορείτε να εκτυπώσετε μόνον αρχεία γραμμένα στη γλώσσα του.

Οι χρήστες συνήθως νομίζουν πως μπορούν να εκτυπώσουν απλό κείμενο σε όλους τους εκτυπωτές που είναι εγκατεστημένοι στο σύστημα τους. Τα προγράμματα που χρησιμοποιούν το LPD για να εκτυπώσουν, κάνουν ακριβώς την ίδια υπόθεση. Αν προσπαθείτε να εγκαταστήσετε έναν τέτοιο εκτυπωτή και θέλετε να μπορείτε να τυπώνετε εργασίες στην γλώσσα του εκτυπωτή αλλά *και* σε απλό κείμενο, σας συνιστούμε να προσθέσετε ένα επιπλέον βήμα στην διαδικασία εγκατάστασης που περιγράψαμε παραπάνω: Εγκαταστήστε ένα πρόγραμμα αυτόματης μετατροπής από απλό κείμενο σε PostScript (ή σε άλλη γλώσσα εκτυπωτή). Η ενότητα Συμβατότητα Εργασιών Απλού Κειμένου σε εκτυπωτές PostScript® εξηγεί πως να ενεργήσετε.

16.3.1.5.1. Ονοματοδότηση Εκτυπωτή

Το πρώτο (εύκολο) βήμα είναι να επιλέξετε όνομα για τον εκτυπωτή σας. Δεν έχει σημασία αν θα προτιμήσετε ένα λειτουργικό ή κάποιο εξωτικό όνομα αφού μπορείτε επίσης να προσθέσετε και μερικά παρωνύμια (aliases) για τον ίδιο εκτυπωτή.

Τουλάχιστον ένας από τους εκτυπωτές που αναφέρονται στο /etc/printcap θα πρέπει να έχει το παρωνύμιο `lp`. Αυτή είναι η ονομασία του προεπιλεγμένου εκτυπωτή. Εάν οι χρήστες δεν έχουν την μεταβλητή περιβάλλοντος `PRINTER` και δεν αναφέρουν κάποιο όνομα εκτυπωτή στην γραμμή εντολών με οποιαδήποτε εντολή LPD, τότε ο `lp` θα είναι ο προεπιλεγμένος εκτυπωτής για τις εκτυπώσεις τους.

Επίσης, είναι κοινή πρακτική το τελευταίο alias του εκτυπωτή να είναι μια πλήρης περιγραφή του εκτυπωτή, που να περιλαμβάνει τον κατασκευαστή και το μοντέλο.

Αφού επιλέξετε μια ονομασία και μερικά συνήθη παρωνύμια, καταχωρίστε τα στο αρχείο /etc/printcap. Το όνομα του εκτυπωτή θα πρέπει να αναφέρεται πρώτο στο αριστερό άκρο. Διαχωρίστε κάθε παρωνύμιο με μια κάθετη μπάρα και τοποθετήστε μια άνω-κάτω τελεία μετά το τελευταίο παρωνύμιο.

Στο ακόλουθο παράδειγμα, ξεκινάμε με ένα εντελώς βασικό /etc/printcap που ορίζει δύο εκτυπωτές (έναν εκτυπωτή γραμμής Diablo 630 και έναν εκτυπωτή PostScript® laser Panasonic KX-P4455):

```
#
#  /etc/printcap for host rose
#
rattan|line|diablo|lp|Diablo 630 Line Printer:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:
```

Σε αυτό το παράδειγμα, ο πρώτος εκτυπωτής ονομάζεται `rattan` και έχει ως παρωνύμια τα `line`, `diablo`, `lp`, και `Diablo 630 Line Printer`. Από τη στιγμή που έχει το παρωνύμιο `lp`, είναι και ο προεπιλεγμένος εκτυπωτής. Ο δεύτερος ονομάζεται `bamboo`, και έχει ως παρωνύμια τα `ps`, `PS`, `S`, `panasonic`, και `Panasonic KX-P4455 PostScript v51.4`.

16.3.1.5.2. Παρεμπόδιση Σελίδων Κεφαλίδας

Το σύστημα παροχέτευσης LPD, από προεπιλογή, εκτυπώνει μια *σελίδα κεφαλίδας* για κάθε εργασία. Η σελίδα κεφαλίδας περιλαμβάνει το όνομα χρήστη που αιτήθηκε την εργασία, τον υπολογιστή από τον οποίον προήλθε η εργασία, και το όνομα της εργασίας, με μεγάλους όμορφους χαρακτήρες. Δυστυχώς αυτό το πρόσθετο κείμενο ακολουθεί την διαδικασία αποσφαλμάτωσης της εγκατάστασης ενός απλού εκτυπωτή, επομένως θα παρεμποδίσουμε τις σελίδες κεφαλίδας.

Για την παρεμπόδιση των σελίδων κεφαλίδας, προσθέστε την ικανότητα `sh` στην καταχώριση για τον εκτυπωτή στο αρχείο /etc/printcap. Εδώ βλέπετε ένα παράδειγμα του /etc/printcap με προσθήκη της `sh`:

```
#
#  /etc/printcap for host rose - no header pages anywhere
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:
```

Παρατηρήστε πως χειριστήκαμε σωστά τη μορφή: η πρώτη γραμμή ξεκινά στην αριστερή στήλη, και οι ακόλουθες γραμμές είναι στοιχισμένες (indented). Κάθε γραμμή καταχώρισης (εκτός από την τελευταία) τελειώνει με μια αριστερόστροφη κάθετο.

16.3.1.5.3. Δημιουργία Καταλόγου Παροχέτευσης

Το επόμενο βήμα στον απλό τρόπο εγκατάστασης είναι η δημιουργία ενός *καταλόγου παροχέτευσης (spool)*, όπου θα φιλοξενούνται οι εργασίες εκτύπωσης έως ότου να εκτυπωθούν και όπου επίσης φυλάσσονται και κάποια άλλα βοηθητικά αρχεία του συστήματος εκτύπωσης.

Λόγω της μεταβαλλόμενης φύσης των καταλόγων παροχέτευσης, συνηθίζεται να τοποθετούνται κάτω από τον κατάλογο /var/spool. Δεν είναι αναγκαίο να παίρνετε αντίγραφα ασφαλείας των καταλόγων παροχέτευσης. Η επαναδημιουργία τους είναι τόσο απλή όσο να τρέξουμε την εντολή mkdir(1).

Είναι επίσης συνηθισμένο να ονομάζεται ο κατάλογος με το ίδιο όνομα με τον εκτυπωτή, όπως φαίνεται παρακάτω:

```
# mkdir /var/spool/printer-name
```

Ωστόσο, αν έχετε αρκετούς εκτυπωτές στο δίκτυο, ίσως επιθυμείτε να τοποθετήσετε τους καταλόγους παροχέτευσης κάτω από ένα μοναδικό κατάλογο που θα χρησιμοποιείται αποκλειστικά για εκτυπώσεις με το LPD. Θα κάνουμε ακριβώς αυτό για τα παραδείγματα μας με τους εκτυπωτές `rattan` και `bamboo`:

```
# mkdir /var/spool/lpd
# mkdir /var/spool/lpd/rattan
```

```
# mkdir /var/spool/lpd/bamboo
```

Εάν οι εργασίες των χρηστών περιέχουν προσωπικά δεδομένα, μπορεί να θέλετε να προστατέψετε τον κατάλογο παροχέτευσης με κάποιο τρόπο, ώστε να μην είναι δημόσια προσβάσιμος. Οι κατάλογοι παροχέτευσης θα πρέπει να ανήκουν και να είναι αναγνώσιμοι, εγγράψιμοι και με δυνατότητα αναζήτησης από τον χρήστη daemon και από την ομάδα daemon, από κανέναν άλλο. Για τους εκτυπωτές του παραδείγματος:

```
# chown daemon:daemon /var/spool/lpd/rattan
# chown daemon:daemon /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan
# chmod 770 /var/spool/lpd/bamboo
```

Τέλος, πρέπει να ενημερώσετε το LPD για αυτούς τους καταλόγους χρησιμοποιώντας το αρχείο /etc/printcap. Προσδιορίστε την διαδρομή του καταλόγου παροχέτευσης με την ικανότητα `sd`:

```
#
#  /etc/printcap for host rose - added spooling directories
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:
```

Σημειώστε πως το όνομα του εκτυπωτή ξεκινά στην πρώτη στήλη, ενώ όλες οι άλλες καταχωρίσεις που περιγράφουν τον εκτυπωτή θα πρέπει να είναι στοιχισμένες και κάθε τέλος γραμμής να φέρει χαρακτήρα διαφυγής με αριστερόστροφη κάθετο.

Εάν δεν προσδιορίσετε τον κατάλογο παροχέτευσης μέσω του `sd`, τότε το σύστημα παροχέτευσης θα χρησιμοποιήσει τον προεπιλεγμένο /var/spool/lpd.

16.3.1.5.4. Αναγνώριση της Συσκευής Εκτύπωσης

Στην ενότητα Ρυθμίσεις Hardware αναγνωρίσαμε τη θύρα, και κατά συνέπεια την καταχώριση του καταλόγου /dev που θα χρησιμοποιήσει το FreeBSD για να επικοινωνήσει με τον εκτυπωτή. Τώρα, θα δώσουμε στο LPD αυτή την πληροφορία. Όταν το σύστημα παροχέτευσης έχει μια εργασία να εκτυπώσει, θα ανοίξει αυτή την ειδική συσκευή για λογαριασμό του προγράμματος φίλτρου (που είναι υπεύθυνο για το πέρασμα των δεδομένων στον εκτυπωτή).

Προσδιορίστε την διαδρομή της καταχώρισης /dev στο αρχείο /etc/printcap χρησιμοποιώντας την ικανότητα `lp`.

Στο τρέχον παράδειγμα μας, ας υποθέσουμε ότι ο `rattan` είναι στην πρώτη παράλληλη θύρα, και ο `bamboo` είναι στην έκτη σειριακή πόρτα. Οι νέες καταχωρίσεις στο /etc/printcap θα είναι:

```
#
#  /etc/printcap for host rose - identified what devices to use
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyu5:
```

Αν δεν καθορίσετε σε κάποιον εκτυπωτή την ικανότητα `lp` στο αρχείο /etc/printcap, το LPD χρησιμοποιεί από προεπιλογή το /dev/lp. Το /dev/lp δεν υπάρχει την δεδομένη στιγμή στο FreeBSD.

Εάν ο εκτυπωτής που εγκαθιστάτε είναι συνδεδεμένος σε παράλληλη θύρα, διαβάστε απευθείας την ενότητα με τίτλο Εγκατάσταση Φίλτρου Κειμένου. Διαφορετικά, ακολουθήστε προσεκτικά τις οδηγίες που ακολουθούν στην επόμενη ενότητα.

16.3.1.5.5. Ρυθμίσεις Παραμέτρων Επικοινωνίας του Spooler

Για εκτυπωτές σε σειριακή πόρτα, το LPD μπορεί να ρυθμίσει την ταχύτητα σε bps, το parity, και άλλες παραμέτρους σειριακής επικοινωνίας για λογαριασμό του προγράμματος φίλτρου που στέλνει δεδομένα στον εκτυπωτή. Αυτό είναι πλεονέκτημα γιατί:

- Σας επιτρέπει να δοκιμάσετε διάφορες παραμέτρους επικοινωνίας προσθέτοντας τις απλά με επεξεργασία του αρχείου /etc/printcap. Δεν χρειάζεται να επαναμεταγλωττίσετε το πρόγραμμα φίλτρου.
- Επιτρέπει στο σύστημα παροχέτευσης να χρησιμοποιεί το ίδιο πρόγραμμα για πολλαπλούς εκτυπωτές, οι οποίοι μπορεί να έχουν διαφορετικές σειριακές ρυθμίσεις επικοινωνίας.

Οι ακόλουθες ικανότητες του /etc/printcap ελέγχουν τις παραμέτρους σειριακής επικοινωνίας των συσκευών που αναφέρονται στην ικανότητα `lp`:

`br#bps-rate`
: Ορίζει την ταχύτητα επικοινωνίας της συσκευής σε *bps-rate*, όπου το *bps-rate* μπορεί να είναι 50, 75, 110, 134, 150, 200, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, ή 115200 bits-per-second.

`ms#stty-mode`
: Ορίζει τις επιλογές της συσκευής τερματικού μετά το άνοιγμα της συσκευής. Η stty(1) εξηγεί τις διαθέσιμες επιλογές.

Όταν το LPD ανοίγει την συσκευή που ορίζεται από την ικανότητα `lp`, υιοθετεί τα χαρακτηριστικά της συσκευής με ικανότητα `ms#`. Έχουν ιδιαίτερο ενδιαφέρον οι καταστάσεις λειτουργίας `parenb`, `parodd`, `cs5`, `cs6`, `cs7`, `cs8`, `cstopb`, `crtscts`, και `ixon`, που εξηγούνται στην σελίδα βοηθείας stty(1).

Ας προσθέσουμε στο παράδειγμα μας έναν εκτυπωτή στην έκτη σειριακή θύρα. Θα θέσουμε την ταχύτητα bps σε 38400. Για την κατάσταση λειτουργίας θα θέσουμε , no parity με `-parenb`,

χαρακτήρες 8-bit με `cs8`, no modem control με `clocal` και έλεγχο ροής μέσω hardware με `crtscts`:

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:
```

16.3.1.5.6. Εγκατάσταση Φίλτρου Κειμένου

Τώρα είμαστε έτοιμοι να πούμε στο LPD ποιο φίλτρο κειμένου να χρησιμοποιήσει για να στείλει εργασίες στον εκτυπωτή. Το φίλτρο κειμένου, γνωστό και ως *φίλτρο εισόδου*, είναι ένα πρόγραμμα που εκτελεί το LPD όταν υπάρχει εργασία προς εκτύπωση. Όταν το LPD εκτελεί το φίλτρο κειμένου για κάποιον εκτυπωτή, θέτει την standard input του φίλτρου στην εργασία εκτύπωσης, και την standard output στην συσκευή του εκτυπωτή που ορίζεται με την ικανότητα `lp`. Το φίλτρο αναμένεται να αναγνώσει την εργασία από την standard input, να εκτελέσει όλες τις απαραίτητες μεταγλωττίσεις για τον εκτυπωτή, και να γράψει το αποτέλεσμα στην standard output, το οποίο και θα εκτυπωθεί. Για περισσότερες πληροφορίες για τα φίλτρα κειμένου, δείτε την ενότητα Φίλτρα.

Για την απλή εγκατάσταση των εκτυπωτών μας, το φίλτρο κειμένου μπορεί να είναι ένα μικρό shell script που απλά θα εκτελεί την εντολή `/bin/cat` για να στέλνει εργασίες στον εκτυπωτή. Το FreeBSD έρχεται με άλλο ένα φίλτρο, το lpf που χειρίζεται δυνατότητες backspacing και υπογράμμισης για εκτυπωτές που ίσως να μην χειρίζονται σωστά αυτές τις λειτουργίες. Και φυσικά, μπορείτε να χρησιμοποιήσετε οποιοδήποτε άλλο πρόγραμμα φίλτρου επιθυμείτε. Το φίλτρο `lpf` περιγράφεται λεπτομερώς στην ενότητα lpf: ένα Φίλτρο Κειμένου.

Θα ξεκινήσουμε δημιουργώντας το shell script /usr/local/libexec/if-simple σαν ένα απλό φίλτρο κειμένου. Τοποθετήστε το ακόλουθο κείμενο στο αρχείο χρησιμοποιώντας τον κειμενογράφο που προτιμάτε:

```
#!/bin/sh
#
# if-simple - Simple text input filter for lpd
# Installed in /usr/local/libexec/if-simple
#
# Simply copies stdin to stdout.  Ignores all filter arguments.

/bin/cat && exit 0
exit 2
```

Κάντε το αρχείο εκτελέσιμο:

```
# chmod 555 /usr/local/libexec/if-simple
```

Και ενημερώστε το LPD να το χρησιμοποιήσει, ορίζοντας το με την ικανότητα `if` στο αρχείο /etc/printcap. Θα το προσθέσουμε στους δύο εκτυπωτές από το προηγούμενο παράδειγμα στο /etc/printcap:

```
#
#  /etc/printcap for host rose - added text filter
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:\
        :if=/usr/local/libexec/if-simple:
```

Μπορείτε να βρείτε ένα αντίγραφο του script if-simple στον κατάλογο /usr/shared/examples/printing.

16.3.1.5.7. Ενεργοποίηση του LPD

Το lpd(8) εκτελείται από το /etc/rc, και ελέγχεται από την μεταβλητή `lpd_enable`. Η μεταβλητή αυτή έχει προεπιλεγμένη τιμή `NO`. Αν δεν το έχετε κάνει ακόμα, προσθέστε την ακόλουθη γραμμή:

```
lpd_enable="YES"
```

στο αρχείο /etc/rc.conf, και επανεκκινήστε το σύστημα σας, ή απλά εκτελέστε το lpd(8).

```
# lpd
```

16.3.1.5.8. Δοκιμή του Spooler

Φτάσατε στο τέλος της απλής εγκατάστασης του LPD. Θα αφήσουμε για αργότερα τα συγχαρητήρια, αφού ακόμη θα πρέπει να ελέγξουμε την εγκατάσταση και να διορθώσουμε οποιοδήποτε πρόβλημα έχει προκύψει. Για να ελέγξετε την εγκατάσταση προσπαθήστε να εκτυπώσετε κάτι. Για να εκτυπώσετε με το σύστημα LPD, χρησιμοποιήστε την εντολή lpr(1), η οποία αποστέλλει μία εργασία προς εκτύπωση.

Μπορείτε να συνδυάσετε την lpr(1) με το πρόγραμμα lptest(1), για το οποίο κάναμε μια εισαγωγή στην ενότητα Έλεγχος Επικοινωνίας του Εκτυπωτή, για τον έλεγχο κειμένου.

Για τον έλεγχο μιας απλής εγκατάστασης LPD:

Πληκτρολογήστε:

```
# lptest 20 5 | lpr -Pprinter-name
```

Όπου *printer-name* είναι το όνομα ενός εκτυπωτή (ή το alias) που αναφέρεται στο /etc/printcap. Για να ελέγξετε τον προεπιλεγμένο εκτυπωτή, πληκτρολογήστε lpr(1) χωρίς το πρόθεμα `-P`. Αν ο

εκτυπωτής σας χρησιμοποιεί PostScript®, πρέπει να στείλετε ένα πρόγραμμα PostScript®, αντί να χρησιμοποιήσετε το lptest(1). Για να τα καταφέρετε, τοποθετήστε το πρόγραμμα σε ένα αρχείο και πληκτρολογήστε `lpr file`.

Σε έναν εκτυπωτή PostScript®, η εκτύπωση θα είναι το αποτέλεσμα του προγράμματος που στείλατε. Αν χρησιμοποιείτε το lptest(1), τότε το αποτέλεσμα θα μοιάζει με το ακόλουθο:

```
!"#$%&'()*+,-./01234
"#$%&'()*+,-./012345
#$%&'()*+,-./0123456
$%&'()*+,-./01234567
%&'()*+,-./012345678
```

Για περαιτέρω έλεγχο του εκτυπωτή, δοκιμάστε να κατεβάσετε μεγαλύτερα προγράμματα (για εκτυπωτές που χρησιμοποιούν γλώσσα προγραμματισμού) ή τρέξτε το lptest(1) με διαφορετικά προθέματα. Για παράδειγμα, η εντολή `lptest 80 60` θα παράγει 60 γραμμές των 80 χαρακτήρων η καθεμία.

Αν ο εκτυπωτής δεν δουλεύει, δείτε την ενότητα Εντοπισμός Βλαβών.

16.4. Ρυθμίσεις Εκτυπωτών για Προχωρημένους

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών για τις σειριακές θύρες μετονομάστηκαν από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την τεκμηρίωση που ακολουθεί με βάση αυτές τις αλλαγές.

Αυτή η ενότητα περιγράφει φίλτρα για την εκτύπωση ειδικής μορφής αρχείων, σελίδων κεφαλίδας, για εκτυπώσεις μέσω δικτύου, καθώς και για τον έλεγχο πρόσβασης και την καταμέτρηση χρήσης των εκτυπωτών.

16.4.1. Φίλτρα

Αν και το LPD μπορεί να χειριστεί πρωτόκολλα δικτύων, λίστες αναμονής, έλεγχο πρόσβασης, και άλλες παραμέτρους των εκτυπώσεων, το κύριο μέρος της *πραγματικής* εργασίας γίνεται με τα *φίλτρα*. Τα φίλτρα είναι προγράμματα που επικοινωνούν με τον εκτυπωτή και χειρίζονται τις εξαρτήσεις της συσκευής και άλλες ειδικές απαιτήσεις της. Στην απλή εγκατάσταση εκτυπωτή, εγκαταστήσαμε ένα φίλτρο απλού κειμένου ιδιαίτερα απλής μορφής, που θα πρέπει να δουλεύει με τους περισσότερους εκτυπωτές (ενότητα Εγκατάσταση Φίλτρου Κειμένου).

Ωστόσο, για να μπορέσετε να εκμεταλλευτείτε τις δυνατότητες μετατροπών μορφής, ελέγχου πρόσβασης και καταμέτρησης, και τυχόν ειδικές δυνατότητες του εκτυπωτή σας, θα πρέπει να καταλάβετε πως δουλεύουν τα φίλτρα. Σε τελική ανάλυση, θα είναι ευθύνη των φίλτρων να χειρίζονται όλες αυτές τις παραμέτρους. Τα κακά νέα είναι πως τις περισσότερες φορές θα πρέπει να παρέχετε *εσείς οι ίδιοι* τα φίλτρα σας. Τα καλά νέα είναι πως γενικώς υπάρχουν αρκετά διαθέσιμα, και αν δεν υπάρχουν, είναι σχετικά εύκολο να τα γράψετε.

Επίσης, το FreeBSD διατίθεται με ένα φίλτρο, το /usr/libexec/lpr/lpf, που δουλεύει με πολλούς εκτυπωτές που μπορούν να εκτυπώσουν απλό κείμενο. (Χειρίζεται backspacing και tabs στο αρχείο, και κάνει καταμέτρηση, αλλά τίποτα περισσότερο.) Υπάρχουν, επίσης, διάφορα άλλα φίλτρα και συστατικά τους στην Συλλογή των Ports του FreeBSD.

Σε αυτή την ενότητα θα βρείτε: :

- Η ενότητα Πως δουλεύουν τα Φίλτρα, προσπαθεί να δώσει μια γενική άποψη για τις αρμοδιότητες των φίλτρων στις διεργασίες εκτύπωσης. Θα πρέπει να διαβάσετε αυτή την ενότητα για να μπορείτε να καταλάβετε τι "πραγματικά" συμβαίνει όταν το LPD χρησιμοποιεί φίλτρα. Αυτές οι γνώσεις θα σας βοηθήσουν να προλαμβάνετε και να αποσφαλματώνετε προβλήματα που μπορούν να συμβούν καθώς εγκαθιστάτε όλο και περισσότερα φίλτρα σε κάθε εκτυπωτή σας.
- Το LPD αναμένει πως κάθε εκτυπωτής είναι ικανός, από προεπιλογή, να εκτυπώσει απλό κείμενο. Αυτό όμως είναι πρόβλημα για εκτυπωτές PostScript® (ή άλλους που βασίζονται σε γλώσσες προγραμματισμού) οι οποίοι δεν μπορούν να εκτυπώσουν άμεσα απλό κείμενο. Η ενότητα Συμβατότητα Εργασιών Απλού Κειμένου σε εκτυπωτές PostScript® σας εξηγεί τι θα πρέπει να κάνετε για να ξεπεράσετε αυτό το πρόβλημα. Θα πρέπει να διαβάσετε αυτή την ενότητα αν έχετε εκτυπωτή PostScript®.
- Το PostScript® είναι δημοφιλής μορφή εξόδου για πολλά προγράμματα. Μερικοί άνθρωποι προτιμούν και να γράφουν κατευθείαν σε κώδικα PostScript®. Δυστυχώς, οι εκτυπωτές PostScript® έχουν μεγάλο κόστος. Η ενότητα Προσομοίωση PostScript® για εκτυπωτές που δεν το υποστηρίζουν εξηγεί λεπτομερώς πως να μετατρέψετε ένα φίλτρο κειμένου για εκτυπωτές ώστε να λαμβάνει και να τυπώνει δεδομένα PostScript® σε εκτυπωτές που *δεν είναι PostScript*®. Θα πρέπει να διαβάσετε αυτήν την ενότητα αν είστε κάτοχος εκτυπωτή που δεν υποστηρίζει PostScript®.
- Η ενότητα Φίλτρα Μετατροπής περιγράφει μια αυτοματοποιημένη διαδικασία για την μετατροπή αρχείων ειδικής μορφής, όπως δεδομένα γραφικών ή στοιχειοθεσίας, σε μια μορφή κατανοητή από τον εκτυπωτή σας. Μετά την ανάγνωση αυτής της ενότητας, θα πρέπει να είστε σε θέση να ρυθμίσετε τους εκτυπωτές σας με τέτοιο τρόπο ώστε πληκτρολογώντας `lpr -t` οι χρήστες σας να μπορούν να εκτυπώσουν δεδομένα troff, ή με `lpr -d` δεδομένα TeX DVI, ή με `lpr -v` να εκτυπώνουν εικόνες δεδομένων ράστερ, και ούτω καθεξής. Σας συμβουλεύουμε να διαβάσετε αυτή την ενότητα.
- Η ενότητα Φίλτρα Εξόδου περιγράφει ένα χαρακτηριστικό του LPD που δεν χρησιμοποιείται συχνά: τα φίλτρα εξόδου. Μπορείτε να προσπεράσετε αυτή την ενότητα, εκτός αν τυπώνετε σελίδες κεφαλίδας (δείτε τις Σελίδες Κεφαλίδας).
- Η ενότητα lpf: ένα Φίλτρο Κειμένου περιγράφει το `lpf`, ένα πραγματικά πλήρες, αν και απλό, φίλτρο κειμένου για εκτυπωτές γραμμής (και εκτυπωτές laser που μπορούν να λειτουργήσουν και ως εκτυπωτές γραμμής) που περιέχεται στο FreeBSD. Αν χρειάζεστε ένα γρήγορο τρόπο για να κάνετε την καταμέτρηση σελίδων να δουλεύει σε απλό κείμενο, ή αν έχετε κάποιον εκτυπωτή που βγάζει καπνούς όταν βλέπει χαρακτήρες backspace, θα πρέπει οπωσδήποτε να εξετάσετε την περίπτωση του `lpf`.

Μπορείτε να βρείτε αντίγραφο των διάφορων scripts που αναφέρονται παρακάτω, στον κατάλογο /usr/shared/examples/printing.

16.4.1.1. Πως Δουλεύουν τα Φίλτρα

Όπως αναφέραμε προηγουμένως, φίλτρο είναι ένα εκτελέσιμο πρόγραμμα που ενεργοποιείται από το LPD για να χειρίζεται το τμήμα της επικοινωνίας με τον εκτυπωτή που εξαρτάται από τον τύπο της ίδιας της συσκευής.

Όταν το LPD θέλει να εκτυπώσει ένα αρχείο μιας εργασίας, ξεκινά το πρόγραμμα του φίλτρου. Θέτει ως standard input του φίλτρου το αρχείο που πρέπει να εκτυπωθεί, ως standard output τον ίδιο τον εκτυπωτή και ως standard error το αρχείο αναφοράς σφαλμάτων (αναφέρεται στην ικανότητα `lf` του /etc/printcap, ή από προεπιλογή το /dev/console).

Το φίλτρο που θα ξεκινήσει το LPD καθώς και οι παράμετροι του φίλτρου, εξαρτώνται από το τι έχετε δηλώσει στο αρχείο /etc/printcap και από το τι παραμέτρους έχει καθορίσει ο ίδιος ο χρήστης για την εργασία με την γραμμή εντολής lpr(1). Για παράδειγμα, αν ο χρήστης πληκτρολογήσει `lpr -t`, το LPD θα ξεκινήσει το φίλτρο troff, που υποδηλώνεται με την ικανότητα `tf` για τον εκτυπωτή προορισμού. Αν ο χρήστης επιθυμεί να εκτυπώσει απλό κείμενο, θα ξεκινήσει το φίλτρο `if` (αυτό πράγματι ισχύει τις περισσότερες φορές: δείτε τα Φίλτρα Εξόδου για λεπτομέρειες).

Υπάρχουν τρεις τύποι φίλτρων που μπορείτε να προσδιορίσετε στο /etc/printcap:

- Το *φίλτρο κειμένου*, επονομαζόμενο και ως *φίλτρο εισόδου* στην τεκμηρίωση του LPD, χειρίζεται εκτυπώσεις κανονικού κειμένου. Θεωρήστε το ως το προεπιλεγμένο φίλτρο. Το LPD αναμένει πως όλοι οι εκτυπωτές, από προεπιλογή, είναι σε θέση να εκτυπώσουν απλό κείμενο, και είναι δουλειά του φίλτρου κειμένου να βεβαιωθεί ότι τα backspaces, τα tabs, και όλοι οι άλλοι ειδικοί χαρακτήρες δεν πρόκειται να προβληματίσουν τον εκτυπωτή. Εάν βρίσκεστε σε ένα περιβάλλον όπου θα πρέπει να καταμετρήσετε την χρήση των εκτυπωτών, το φίλτρο κειμένου θα πρέπει επίσης να καταμετρήσει τις εκτυπωμένες σελίδες, συνήθως μετρώντας τον αριθμό των εκτυπωμένων γραμμών και συγκρίνοντας τον με τον αριθμό των γραμμών που υποστηρίζει ο εκτυπωτής ανά σελίδα. Το φίλτρο κειμένου ξεκινά με την ακόλουθη λίστα παραμέτρων:

  `filter-name` [-c] -w*width* -l*length* -i*indent* -n *login* -h *host acct-file*

  όπου

  `-c`

  εμφανίζεται αν η εργασία έχει αποσταλεί με `lpr -l`

  `width`

  είναι η τιμή από την ικανότητα `pw` (πλάτος σελίδας - page width) όπως προσδιορίζεται στο /etc/printcap, με προεπιλεγμένη τιμή το 132

  `length`

  είναι η τιμή από την ικανότητα `pl` (μήκος σελίδας - page length), με προεπιλεγμένη τιμή το 66

  `indent`

  είναι το μέγεθος της εσοχής (indentation) από το `lpr -i`, με προεπιλεγμένη τιμή 0

  `login`

  είναι το καταγεγραμμένο όνομα χρήστη που εκτυπώνει το αρχείο

host

είναι το όνομα του υπολογιστή από τον οποίο στάλθηκε η εργασία

acct-file

είναι το όνομα του αρχείου καταμέτρησης από την ικανότητα `af`.

- Ένα *φίλτρο μετατροπής* μετατρέπει ένα αρχείο ειδικής μορφής σε ένα τύπο αρχείου κατάλληλο για εκτύπωση από τον συγκεκριμένο εκτυπωτή. Για παράδειγμα, τα δεδομένα στοιχειοθεσίας ditroff δεν μπορούν να εκτυπωθούν κατευθείαν, αλλά μπορείτε να εγκαταστήσετε ένα φίλτρο μετατροπής αρχείων ditroff, ώστε να μετατρέψετε τα δεδομένα ditroff σε μια μορφή που ο εκτυπωτής να μπορεί να αφομοιώσει και να τυπώσει. Θα μάθετε περισσότερα στην ενότητα Φίλτρα Μετατροπής. Τα φίλτρα μετατροπής επίσης χρειάζονται για να κάνετε αρίθμηση/καταμέτρηση, αν χρειάζεστε καταμέτρηση των εκτυπώσεων σας. Τα φίλτρα μετατροπής ξεκινούν με τις ακόλουθες παραμέτρους:

  `filter-name` -x*pixel-width* -y*pixel-height* -n *login* -h *host acct-file* όπου *pixel-width* είναι η τιμή από την ικανότητα px (προεπιλεγμένη τιμή 0) και *pixel-height* είναι η τιμή από την ικανότητα py (προεπιλεγμένη τιμή 0).

- Το *φίλτρο εξόδου* χρησιμοποιείται μόνον αν δεν υπάρχει φίλτρο κειμένου, ή αν είναι ενεργοποιημένες οι σελίδες κεφαλίδας. Διαβάστε τη σχετική ενότητα Φίλτρα Εξόδου, αν και από την εμπειρία μας μπορούμε να σας πούμε ότι χρησιμοποιούνται σπάνια. Υπάρχουν μόνο δύο παράμετροι για τα φίλτρα εξόδου:

  `filter-name` -w*width* -l*length* οι οποίες είναι πανομοιότυπες με τις παραμέτρους `-w` και `-l` των φίλτρων κειμένου.

Τα φίλτρα θα πρέπει επίσης να *τερματίζουν* με κάποια από τις ακόλουθες καταστάσεις εξόδου:

exit 0

Αν το φίλτρο τύπωσε επιτυχώς το αρχείο.

exit 1

Αν το φίλτρο απέτυχε να τυπώσει το αρχείο, αλλά θέλει το LPD να προσπαθήσει να εκτυπώσει το αρχείο ξανά. Το LPD θα ξεκινήσει ξανά το φίλτρο αν γίνει έξοδος με αυτή την κατάσταση.

exit 2

Αν το φίλτρο απέτυχε να εκτυπώσει το αρχείο και δεν θέλει το LPD να προσπαθήσει ξανά. Το LPD θα απορρίψει το αρχείο.

Το φίλτρο κειμένου που έρχεται με την κανονική έκδοση του FreeBSD, /usr/libexec/lpr/lpf, εκμεταλλεύεται τις παραμέτρους πλάτους και μήκους σελίδας για να προσδιορίσει πότε να αποστείλει το form feed και πως να κάνει καταμέτρηση. Χρησιμοποιεί τις παραμέτρους για login, host, και αρχείου καταμέτρησης για να δημιουργήσει τις σχετικές εγγραφές καταμέτρησης.

Αν είστε στη διαδικασία επιλογής φίλτρων, ελέγξτε αν είναι συμβατά με το LPD. Αν είναι συμβατά, τότε πρέπει να υποστηρίζουν την λίστα παραμέτρων που περιγράψαμε προηγουμένως. Αν σχεδιάζετε να γράψατε τα δικά σας φίλτρα γενικής χρήσης, τότε πρέπει να τα κάνετε να υποστηρίζουν την ίδια λίστα παραμέτρων και κωδικών εξόδου.

16.4.1.2. Συμβατότητα Εργασιών Απλού Κειμένου σε Εκτυπωτές PostScript®

Αν είστε ο μοναδικός χρήστης του Η/Υ σας και του εκτυπωτή PostScript® (ή άλλης γλώσσας εκτυπωτών), και είστε σίγουροι πως δεν πρόκειται να στείλετε ποτέ εκτυπώσεις απλού κειμένου στον εκτυπωτή σας και πως δεν θα χρησιμοποιήσετε τις υπηρεσίες των διαφόρων προγραμμάτων σας που θα θελήσουν να στείλουν απλό κείμενο στον εκτυπωτή σας, τότε δεν χρειάζεται να ασχοληθείτε καθόλου με αυτή την ενότητα.

Αλλά, αν επιθυμείτε να στείλετε τόσο εργασίες PostScript® όσο και απλού κειμένου στον εκτυπωτή σας, τότε σας προτρέπουμε να προσθέσετε κάποιες ρυθμίσεις στην εγκατάσταση σας. Για να γίνει αυτό, θα πρέπει το φίλτρο κειμένου να ανιχνεύει αν η τρέχουσα εργασία είναι απλό κείμενο ή PostScript®. Όλες οι εργασίες PostScript® πρέπει να ξεκινούν με `%!` (αν ο εκτυπωτής σας χρησιμοποιεί άλλη γλώσσα, συμβουλευθείτε την τεκμηρίωση του). Αν είναι αυτοί οι πρώτοι δύο χαρακτήρες, τότε έχουμε PostScript®, και η υπόλοιπη εργασία μπορεί να σταλεί απευθείας στον εκτυπωτή. Αν δεν είναι αυτοί οι πρώτοι δύο χαρακτήρες, τότε το φίλτρο θα μετατρέψει το κείμενο σε PostScript® και θα τυπώσει το αποτέλεσμα.

Πως γίνεται αυτό;

Αν είστε κάτοχος σειριακού εκτυπωτή, ένας καλός τρόπος για να γίνει αυτό εφικτό είναι να εγκαταστήσετε το `lprps`. Το `lprps` είναι ένα φίλτρο εκτύπωσης PostScript® που επικοινωνεί αμφίδρομα με τον εκτυπωτή. Ενημερώνει το αρχείο κατάστασης του εκτυπωτή με αναλυτικές πληροφορίες, ώστε οι χρήστες και οι διαχειριστές να μπορούν να δουν επακριβώς ποια είναι η κατάσταση του εκτυπωτή (όπως `χαμηλή στάθμη toner` ή `πρόβλημα χαρτιού`). Ακόμη πιο σημαντικό είναι πως περιέχει το πρόγραμμα `psif` που ανιχνεύει αν η εισερχόμενη εργασία είναι απλού κειμένου και καλεί το `textps` (ένα άλλο πρόγραμμα που περιέχεται στο `lprps`) να το μετατρέψει σε PostScript®. Τέλος χρησιμοποιείται το `lprps` για να αποστείλει την εργασία στον εκτυπωτή.

Το `lprps` είναι μέρος της Συλλογής των Ports του FreeBSD (δείτε Η Συλλογή των Ports). Φυσικά, μπορείτε να το κατεβάσετε, να το μεταγλωττίσετε και να το εγκαταστήσετε μόνοι σας. Μετά την εγκατάσταση του `lprps`, απλά προσδιορίστε τη διαδρομή προς το πρόγραμμα `psif` που είναι μέρος του `lprps`. Αν εγκαταστήσατε το `lprps` από την Συλλογή των Ports, τότε για τον σειριακό σας εκτυπωτή PostScript® χρησιμοποιήστε την ακόλουθη καταχώριση στο αρχείο /etc/printcap:

```
:if=/usr/local/libexec/psif:
```

Θα πρέπει επίσης να καθορίσετε την ικανότητα `rw` η οποία ορίζει ότι το LPD θα χειρίζεται τον εκτυπωτή σε κατάσταση ανάγνωσης και εγγραφής.

Αν έχετε παράλληλο εκτυπωτή PostScript® (και για το λόγο αυτό δεν μπορείτε να χρησιμοποιήσετε αμφίδρομη επικοινωνία με τον εκτυπωτή, όπως απαιτείται από το `lprps`), μπορείτε να χρησιμοποιήσετε το ακόλουθο shell script ως φίλτρο κειμένου:

```
#!/bin/sh
#
#  psif - Print PostScript or plain text on a PostScript printer
#  Script version; NOT the version that comes with lprps
#  Installed in /usr/local/libexec/psif
```

```
#

IFS="" read -r first_line
first_two_chars=`expr "$first_line" : '\(..\)'`

if [ "$first_two_chars" = "%!" ]; then
    #
    #  PostScript job, print it.
    #
    echo "$first_line" && cat && printf "\004" && exit 0
    exit 2
else
    #
    #  Plain text, convert it, then print it.
    #
    ( echo "$first_line"; cat ) | /usr/local/bin/textps && printf "\004" && exit 0
    exit 2
fi
```

Στο παραπάνω script, το `textps` είναι ένα πρόγραμμα που εγκαταστήσαμε ξεχωριστά για να μετατρέπουμε απλό κείμενο σε PostScript®. Μπορείτε να χρησιμοποιείτε οποιοδήποτε πρόγραμμα μετατροπής από κείμενο- σε-PostScript®. Η Συλλογή των Ports (δείτε Η Συλλογή των Ports) περιέχει επίσης ένα πλήρες πρόγραμμα μετατροπής από κείμενο σε PostScript®, το `a2ps` που ίσως επιθυμείτε να διερευνήσετε.

16.4.1.3. Προσομοίωση PostScript® για Εκτυπωτές που δεν το Υποστηρίζουν

Το PostScript® είναι το *de facto* πρότυπο για στοιχειοθεσία και εκτύπωση υψηλής ποιότητας. Ωστόσο, το PostScript® είναι κάπως *δαπανηρό* πρότυπο. Ευτυχώς, η Aladdin Enterprises παρέχει ένα παρεμφερές ελεύθερο PostScript® που ονομάζεται Ghostscript και δουλεύει άψογα στο FreeBSD. Το Ghostscript διαβάζει τα περισσότερα αρχεία PostScript® και μπορεί να αποδώσει τις σελίδες τους σε μεγάλη γκάμα συσκευών, συμπεριλαμβάνοντας πολλούς τύπους εκτυπωτών που δεν υποστηρίζουν PostScript®. Εγκαθιστώντας το Ghostscript και χρησιμοποιώντας ένα ειδικό φίλτρο κειμένου για τον εκτυπωτή σας, μπορείτε να κάνετε τον κοινό εκτυπωτή σας να λειτουργεί σαν ένας πραγματικός εκτυπωτής PostScript®.

Το Ghostscript βρίσκεται στην Συλλογή των Ports του FreeBSD, και μάλιστα σε πολλές εκδόσεις. Η πιο διαδεδομένη είναι το print/ghostscript-gpl.

Για να κάνετε προσομοίωση PostScript®, πρέπει το φίλτρο κειμένου να ανιχνεύσει αν εκτυπώνετε αρχείο PostScript®. Εάν όχι, τότε το φίλτρο θα περάσει το αρχείο κατευθείαν στον εκτυπωτή. Διαφορετικά, θα χρησιμοποιήσει το Ghostscript για να μετατρέψει αρχικά το αρχείο σε ένα τύπο που θα καταλαβαίνει ο εκτυπωτής.

Ιδού ένα παράδειγμα: το ακόλουθο script είναι ένα φίλτρο κειμένου για εκτυπωτές Hewlett Packard DeskJet 500. Για άλλους εκτυπωτές, αντικαταστήστε το όρισμα `-sDEVICE` στην εντολή `gs` (Ghostscript). (Πληκτρολογήστε `gs -h` για να δείτε την λίστα συσκευών που υποστηρίζει η τρέχουσα εγκατάσταση του Ghostscript.)

```
#!/bin/sh
#
#  ifhp - Print Ghostscript-simulated PostScript on a DeskJet 500
#  Installed in /usr/local/libexec/ifhp

#
#  Treat LF as CR+LF (to avoid the "staircase effect" on HP/PCL
#  printers):
#
printf "\033&k2G" || exit 2

#
#  Read first two characters of the file
#
IFS="" read -r first_line
first_two_chars=`expr "$first_line" : '\(..\)'`

if [ "$first_two_chars" = "%!" ]; then
    #
    #  It is PostScript; use Ghostscript to scan-convert and print it.
    #
    /usr/local/bin/gs -dSAFER -dNOPAUSE -q -sDEVICE=djet500 \
      -sOutputFile=- - && exit 0
else
    #
    #  Plain text or HP/PCL, so just print it directly; print a form feed
    #  at the end to eject the last page.
    #
    echo "$first_line" && cat && printf "\033&l0H" &&
exit 0
fi

exit 2
```

Τέλος, χρειάζεται να ενημερώσετε το LPD για το φίλτρο με την ικανότητα `if`:

```
:if=/usr/local/libexec/ifhp:
```

Αυτό είναι όλο. Μπορείτε να πληκτρολογήσετε `lpr plain.text` και `lpr whatever.ps` και τα δύο θα εκτυπωθούν επιτυχώς.

16.4.1.4. Φίλτρα Μετατροπής

Το επόμενο βήμα μετά την ολοκλήρωση της απλής εγκατάστασης που περιγράψαμε στις Βασικές Ρυθμίσεις Εκτυπωτών, είναι συνήθως η εγκατάσταση φίλτρων μετατροπής για τους τύπους αρχείων που προτιμάτε (εκτός από απλό κείμενο ASCII).

16.4.1.4.1. Γιατί να εγκαταστήσετε Φίλτρα Μετατροπής;

Τα φίλτρα μετατροπής κάνουν την εκτύπωση διαφόρων τύπων αρχείων εύκολη υπόθεση. Για παράδειγμα, ας υποθέσουμε ότι έχουμε να κάνουμε αρκετή εργασία με το σύστημα στοιχειοθεσίας TeX, και ότι έχουμε εκτυπωτή PostScript®. Κάθε φορά που δημιουργούμε ένα αρχείο DVI με το TeX, δεν μπορούμε να εκτυπώσουμε κατευθείαν έως ότου να μετατρέψουμε το αρχείο DVI σε PostScript®. Η ακολουθία εντολών που πρέπει να ακολουθήσουμε είναι:

```
% dvips seaweed-analysis.dvi
% lpr seaweed-analysis.ps
```

Με την χρήση ενός φίλτρου μετατροπής για αρχεία DVI, μπορούμε να αποφύγουμε την μετατροπή που πρέπει να κάνουμε κάθε φορά χειροκίνητα, καλώντας το LPD να κάνει τη δουλειά για μας. Τώρα, κάθε φορά που έχουμε ένα αρχείο DVI, για να το τυπώσουμε χρειάζεται μόνο ένα βήμα:

```
% lpr -d seaweed-analysis.dvi
```

Έχουμε αναθέσει στο LPD να κάνει τη μετατροπή του αρχείου DVI προσθέτοντας του την επιλογή `-d`. Η ενότητα Επιλογές Μορφοποίησης και Μετατροπής περιέχει τους πίνακες επιλογής μετατροπών.

Για κάθε επιλογή μετατροπής που θέλετε να υποστηρίζετε από ένα εκτυπωτή, πρέπει να εγκαταστήσετε ένα *φίλτρο μετατροπής* και να ορίσετε την διαδρομή του στο αρχείο /etc/printcap. Ένα φίλτρο μετατροπής είναι σαν το φίλτρο κειμένου στην απλή εγκατάσταση εκτυπωτή (δείτε την ενότητα Εγκατάσταση Φίλτρου Κειμένου) με μόνη διαφορά πως αντί το φίλτρο να εκτυπώνει απλό κείμενο, μετατρέπει το αρχείο σε μια διαφορετική μορφή ώστε να είναι κατανοητό από τον εκτυπωτή.

16.4.1.4.2. Ποιο Φίλτρο Μετατροπής θα Πρέπει να Εγκαταστήσω;

Θα πρέπει να εγκαθιστάτε τα φίλτρα μετατροπής που νομίζετε πως θα χρησιμοποιήσετε. Αν εκτυπώνετε αρκετά δεδομένα DVI, τότε είναι λογικό να συμπεριλάβετε ένα φίλτρο μετατροπής DVI. Αν εκτυπώνετε συχνά δεδομένα troff, θα θέλετε να εγκαταστήσετε ένα φίλτρο troff.

Ο ακόλουθος πίνακας συνοψίζει τα φίλτρα με τα οποία συνεργάζεται το LPD, τις καταχωρίσεις της αντίστοιχης ικανότητας στο αρχείο /etc/printcap, και πως να τις καλέσετε μέσω της εντολής `lpr`:

Τύπος αρχείου	Ικανότητα /etc/printcap	Παράμετρος εντολής lpr
cifplot	`cf`	`-c`
DVI	`df`	`-d`
plot	`gf`	`-g`
ditroff	`nf`	`-n`
FORTRAN text	`rf`	`-f`
troff	`tf`	`-f`
raster	`vf`	`-v`

Τύπος αρχείου	Ικανότητα /etc/printcap	Παράμετρος εντολής lpr
plain text	`if`	none, `-p`, or `-l`

Στο παράδειγμα μας, αν χρησιμοποιήσουμε `lpr -d` σημαίνει ότι ο εκτυπωτής χρειάζεται την ικανότητα `df` στην καταχώριση του στο /etc/printcap.

Αν και κάποιοι μπορεί να ισχυριστούν το αντίθετο, μερικοί τύποι αρχείων όπως είναι τα κείμενα και γραφικά FORTRAN είναι ξεπερασμένα. Μπορείτε να δώσετε νέα πνοή σε αρχεία αυτού του τύπου (ή και οποιασδήποτε άλλης μορφής εξόδου), εγκαθιστώντας προσαρμοσμένα φίλτρα. Για παράδειγμα, ας υποθέσουμε ότι θα θέλατε να εκτυπώσετε κατευθείαν αρχεία Printerleaf (αρχεία προερχόμενα από το πρόγραμμα επιτραπέζιας τυπογραφίας Interleaf), αλλά δεν θα εκτυπώσετε ποτέ διαγράμματα (plots). Θα μπορούσατε να εγκαταστήσετε ένα φίλτρο μετατροπής αρχείων Printerleaf υπό την ικανότητα `gf` και να εκπαιδεύσετε τους χρήστες σας ότι η εντολή `lpr -g` σημαίνει "τύπωσε αρχεία Printerleaf."

16.4.1.4.3. Εγκατάσταση Φίλτρων Μετατροπών

Από τη στιγμή που τα φίλτρα μετατροπής είναι προγράμματα που δεν ανήκουν στο βασικό σύστημα εγκατάστασης του FreeBSD, είναι πιο σωστό να εγκατασταθούν στον κατάλογο /usr/local. Ένας συνήθης προορισμός των προγραμμάτων αυτών είναι ο κατάλογος /usr/local/libexec, μια που πρόκειται για εξειδικευμένα προγράμματα που εκτελούνται μόνο από το LPD. Οι απλοί χρήστες δεν θα χρειαστεί ποτέ να τα εκτελέσουν.

Για να ενεργοποιήσετε ένα φίλτρο μετατροπής, προσδιορίστε τη διαδρομή του στο αρχείο /etc/printcap, αλλάζοντας την κατάλληλη ικανότητα στον εκτυπωτή που επιθυμείτε να το χρησιμοποιήσετε.

Στο παράδειγμα μας, θα προσθέσουμε το φίλτρο μετατροπής DVI στην καταχώριση μας για τον εκτυπωτή με το όνομα `bamboo`. Ακολουθεί, λοιπόν, το παράδειγμα για το αρχείο /etc/printcap, με την νέα ικανότητα `df` για τον εκτυπωτή `bamboo`:

```
#
#  /etc/printcap for host rose - added df filter for bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Το φίλτρο DVI είναι ένα shell script που ονομάζεται /usr/local/libexec/psdf, το οποίο και παραθέτουμε παρακάτω:

```
#!/bin/sh
#
#  psdf - DVI to PostScript printer filter
#  Installed in /usr/local/libexec/psdf
#
# Invoked by lpd when user runs lpr -d
#
exec /usr/local/bin/dvips -f | /usr/local/libexec/lprps "$@"
```

Αυτό το script τρέχει το `dvips` σε κατάσταση φίλτρου (με την παράμετρο `-f`) στην standard input, από όπου και λαμβάνει την εργασία προς εκτύπωση. Αυτό ξεκινά το φίλτρο εκτύπωσης PostScript® `lprps` (δείτε την ενότητα Συμβατότητα Εργασιών Απλού Κειμένου σε εκτυπωτές PostScript®) δίνοντας του και τις παραμέτρους που πέρασε το LPD στο παραπάνω script. Το `lprps` θα χρησιμοποιήσει αυτές τις παραμέτρους για την καταμέτρηση των εκτυπωμένων σελίδων.

16.4.1.4.4. Ακόμα μερικά Παραδείγματα Φίλτρων Μετατροπής

Από τη στιγμή που δεν υπάρχει αυτοματοποιημένη μέθοδος για την εγκατάσταση των φίλτρων μετατροπής, ας μας επιτραπεί να παρέχουμε μερικά ακόμη παραδείγματα. Μπορείτε να τα χρησιμοποιήσετε σαν οδηγό για την δημιουργία των δικών σας φίλτρων. Αν νομίζετε πως είναι κατάλληλα για την περίπτωση σας μπορείτε να τα χρησιμοποιήσετε και κατευθείαν.

Αυτό το παράδειγμα script είναι ένα φίλτρο μετατροπής ράστερ (αρχείου GIF για την ακρίβεια) για έναν εκτυπωτή Hewlett Packard LaserJet III-Si:

```
#!/bin/sh
#
#  hpvf - Convert GIF files into HP/PCL, then print
#  Installed in /usr/local/libexec/hpvf

PATH=/usr/X11R6/bin:$PATH; export PATH
giftopnm | ppmtopgm | pgmtopbm | pbmtolj -resolution 300 \
    && exit 0 \
    || exit 2
```

Δουλεύει ως εξής: μετατρέπει το αρχείο GIF σε ένα γενικό φορητό τύπο anymap, εν συνεχεία το μετατρέπει σε ένα φορητό τύπο graymap, έπειτα σε ένα φορητό τύπο bitmap, και τέλος το μετατρέπει σε δεδομένα συμβατά με PCL για τον LaserJet.

Εδώ είναι το αρχείο /etc/printcap με μια καταχώριση για έναν εκτυπωτή που χρησιμοποιεί το παραπάνω φίλτρο:

```
#
#  /etc/printcap for host orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sh:sd=/var/spool/lpd/teak:mx#0:\
        :if=/usr/local/libexec/hpif:\
```

```
        :vf=/usr/local/libexec/hpvf:
```

Το ακόλουθο script είναι ένα φίλτρο μετατροπής δεδομένων troff από το σύστημα στοιχειοθεσίας groff για τον εκτυπωτή PostScript® με όνομα bamboo:

```
#!/bin/sh
#
#  pstf - Convert groff's troff data into PS, then print.
#  Installed in /usr/local/libexec/pstf
#
exec grops | /usr/local/libexec/lprps "$@"
```

Το παραπάνω script χρησιμοποιεί πάλι το lprps για να χειριστεί την επικοινωνία με τον εκτυπωτή. Αν ο εκτυπωτής ήταν σε παράλληλη πόρτα τότε θα είχαμε, αντιθέτως, χρησιμοποιήσει το ακόλουθο script:

```
#!/bin/sh
#
#  pstf - Convert groff's troff data into PS, then print.
#  Installed in /usr/local/libexec/pstf
#
exec grops
```

Εδώ είναι η καταχώριση που χρειάζεται να προσθέσουμε στο /etc/printcap για να ενεργοποιήσουμε το φίλτρο:

```
:tf=/usr/local/libexec/pstf:
```

Εδώ είναι ένα παράδειγμα που μας επιτρέπει να εκτυπώσουμε παλαιό κώδικα της FORTRAN. Είναι ένα φίλτρο κειμένου για FORTRAN για οποιονδήποτε εκτυπωτή μπορεί να εκτυπώσει κατευθείαν απλό κείμενο. Θα το εγκαταστήσουμε για έναν εκτυπωτή που ονομάζεται teak:

```
#!/bin/sh
#
# hprf - FORTRAN text filter for LaserJet 3si:
# Installed in /usr/local/libexec/hprf
#

printf "\033&k2G" && fpr && printf "\033&l0H" &&
 exit 0
exit 2
```

Και θα προσθέσουμε αυτή τη γραμμή στο /etc/printcap για να ενεργοποιήσουμε το φίλτρο για τον εκτυπωτή teak:

```
:rf=/usr/local/libexec/hprf:
```

Και ένα τελευταίο κάπως περίπλοκο παράδειγμα: Θα προσθέσουμε ένα φίλτρο DVI στον εκτυπωτή LaserJet `teak` που αναφέραμε προηγούμενα. Καταρχήν το εύκολο μέρος: αναβαθμίζουμε το /etc/printcap με την τοποθεσία όπου βρίσκεται το φίλτρο DVI:

```
:df=/usr/local/libexec/hpdf:
```

Τώρα, το δύσκολο μέρος: η κατασκευή του φίλτρου. Θα χρειαστούμε ένα πρόγραμμα μετατροπής από DVI-σε-LaserJet/PCL. Στην Συλλογή των Ports του FreeBSD (δείτε Συλλογή των Ports) υπάρχει ένα τέτοιο πρόγραμμα: Το όνομα του πακέτου είναι `dvi2xx`. Η εγκατάσταση του πακέτου, μας παρέχει ακριβώς το πρόγραμμα που χρειαζόμαστε, το `dvilj2p`, το οποίο μετατρέπει τον κώδικα DVI σε κώδικα συμβατό με LaserJet IIp, LaserJet III, και LaserJet 2000.

Το `dvilj2p` κάνει το φίλτρο `hpdf` αρκετά περίπλοκο από τη στιγμή που το `dvilj2p` δε μπορεί να διαβάσει από το standard input. Χρειάζεται να δουλέψει με κάποιο όνομα αρχείου. Ακόμη χειρότερα, το όνομα του αρχείου πρέπει να τελειώνει σε .dvi κι επομένως η χρήση του /dev/fd/0 ως standard input είναι προβληματική. Θα μπορούσαμε να αντιμετωπίσουμε το πρόβλημα δημιουργώντας (συμβολικούς) δεσμούς με κάποιο προσωρινό όνομα αρχείου (που να τελειώνει σε .dvi) για το /dev/fd/0, και με αυτό τον τρόπο να εξαναγκάσουμε το `dvilj2p` να διαβάζει από το standard input.

Ακόμη ένα πρόβλημα που προκύπτει είναι το γεγονός πως δεν μπορούμε να χρησιμοποιήσουμε το /tmp για τον προσωρινό δεσμό. Οι συμβολικοί δεσμοί ανήκουν στον χρήστη και στην ομάδα `bin`, ενώ το φίλτρο τρέχει σαν χρήστης `daemon`. Επίσης στον κατάλογο /tmp είναι ενεργό το sticky bit. Το φίλτρο μπορεί να δημιουργήσει το δεσμό, αλλά δεν θα είναι ικανό να τον εξαλείψει και να τον αφαιρέσει από τη στιγμή που αυτός θα ανήκει σε διαφορετικό χρήστη.

Αντίθετα, το φίλτρο θα φτιάξει το συμβολικό link στον τρέχοντα κατάλογο, που είναι ο κατάλογος παροχέτευσης (spooling) (και που προσδιορίζεται από την ικανότητα `sd` στο /etc/printcap). Αυτό είναι το τέλειο μέρος για να δουλεύουν τα φίλτρα, ειδικά λόγω του ότι (μερικές φορές) υπάρχει περισσότερες ελεύθερος χώρος στο δίσκο στον κατάλογο παροχέτευσης (spool) από ότι στο /tmp.

Και τελικά, ιδού το φίλτρο:

```
#!/bin/sh
#
#  hpdf - Print DVI data on HP/PCL printer
#  Installed in /usr/local/libexec/hpdf

PATH=/usr/local/bin:$PATH; export PATH

#
#  Define a function to clean up our temporary files.  These exist
#  in the current directory, which will be the spooling directory
#  for the printer.
#
```

```
cleanup() {
   rm -f hpdf$$.dvi
}

#
#  Define a function to handle fatal errors: print the given message
#  and exit 2.  Exiting with 2 tells LPD to do not try to reprint the
#  job.
#
fatal() {
    echo "$@" 1>&2
    cleanup
    exit 2
}

#
#  If user removes the job, LPD will send SIGINT, so trap SIGINT
#  (and a few other signals) to clean up after ourselves.
#
trap cleanup 1 2 15

#
#  Make sure we are not colliding with any existing files.
#
cleanup

#
#  Link the DVI input file to standard input (the file to print).
#
ln -s /dev/fd/0 hpdf$$.dvi || fatal "Cannot symlink /dev/fd/0"

#
#  Make LF = CR+LF
#
printf "\033&k2G" || fatal "Cannot initialize printer"

#
#  Convert and print.  Return value from dvilj2p does not seem to be
#  reliable, so we ignore it.
#
dvilj2p -M1 -q -e- dfhp$$.dvi

#
#  Clean up and exit
#
cleanup
exit 0
```

16.4.1.4.5. Αυτοματοποιημένες Μετατροπές: Μία Εναλλακτική στα Φίλτρα Μετατροπής

Όλα τα φίλτρα μετατροπής μπορεί να πληρούν το περιβάλλον εκτυπώσεων σας, αλλά υποχρεώνουν τον χρήστη να προσδιορίζει (στην γραμμή εντολών του lpr(1)) ποιό από αυτά θα χρησιμοποιηθεί. Αν οι χρήστες σας δεν είναι ιδιαίτερα εξοικειωμένοι με τους H/Y, το να πρέπει να αναφέρουν κάθε φορά ένα φίλτρο πιθανώς να είναι ενοχλητικό. Είναι ακόμα χειρότερο ωστόσο να γίνει λανθασμένη επιλογή φίλτρου, το οποίο θα εκτελεστεί σε ακατάλληλο για αυτό τύπο αρχείου, και θα προκαλέσει την σπατάλη εκατοντάδων σελίδων χαρτιού.

Αντί να εγκαταστήσετε οποιοδήποτε φίλτρο μετατροπής, μπορεί να θέλετε να δοκιμάσετε να έχετε ένα φίλτρο κειμένου (αφού είναι το προεπιλεγμένο φίλτρο) που να ανιχνεύει τον τύπο του αρχείου που έχει ζητηθεί να εκτυπωθεί και να εκτελεί αυτόματα το κατάλληλο φίλτρο μετατροπής. Εργαλεία σαν το `file` μπορούν να σας βοηθήσουν. Μπορεί να είναι δύσκολο να προσδιοριστούν οι διαφορές μεταξύ *κάποιων* τύπων αρχείων-αλλά, φυσικά, μπορείτε πάντα να παρέχετε φίλτρα μετατροπής ειδικά για αυτές τις περιπτώσεις.

Η Συλλογή των Ports του FreeBSD έχει ένα φίλτρο κειμένου που εκτελεί αυτόματες μετατροπές και ονομάζεται `apsfilter`. Μπορεί να ανιχνεύει απλό κείμενο, PostScript®, DVI και σχεδόν οποιοδήποτε τύπο αρχείου, να εκτελεί την κατάλληλη μετατροπή, και να εκτυπώνει.

16.4.1.5. Φίλτρα Εξόδου

Το σύστημα παροχέτευσης LPD υποστηρίζει έναν ακόμη τύπο φίλτρου που ίσως να μην έχετε εξερευνήσει ακόμα: το φίλτρο εξόδου. Το φίλτρο εξόδου προορίζεται μόνο για εκτύπωση απλού κειμένου, όπως το φίλτρο κειμένου, αλλά με πολλές απλοποιήσεις. Εάν χρησιμοποιείτε φίλτρο εξόδου αλλά όχι φίλτρο κειμένου, τότε:

- Το LPD ξεκινά ένα φίλτρο εξόδου μόνο μια φορά για όλη την εργασία, αντί ένα χωριστό για κάθε αρχείο της εργασίας.
- Το LPD δεν φροντίζει να αναγνωρίσει την αρχή ή το τέλος των αρχείων μέσα στην ίδια την εργασία όταν χρησιμοποιείται το φίλτρο εξόδου.
- Το LPD δεν περνάει στο φίλτρο τα δεδομένα εισόδου του χρήστη ή το όνομα του μηχανήματος, επομένως δεν προορίζεται για καταμέτρηση εκτυπωμένων σελίδων. Το φίλτρο εξόδου δέχεται μόνος τις παραμέτρους: +`filter-name` -w*width* -l*length*

  Όπου το *width* είναι από την ικανότητα `pw` και το *length* είναι από την ικανότητα `pl` για τον συγκεκριμένο εκτυπωτή.

Μην παρασύρεστε από την απλότητα του φίλτρου εξόδου. Αν επιθυμείτε κάθε αρχείο μιας εργασίας να ξεκινά σε μια νέα σελίδα, το φίλτρο εξόδου *δεν κάνει για σας*. Χρησιμοποιήστε ένα φίλτρο κειμένου (γνωστό και ως φίλτρο εισόδου). Δείτε την ενότητα Εγκατάσταση Φίλτρου Κειμένου. Επιπλέον, ένα φίλτρο εξόδου είναι στην πραγματικότητα *πιο περίπλοκο* αφού πρέπει να εξετάζει την ροή των byte που αποστέλλεται προς αυτό για ειδικούς χαρακτήρες flag και πρέπει να στέλνει σήματα στον εαυτό του για λογαριασμό του LPD.

Ωστόσο, ένα φίλτρο εξόδου είναι *αναγκαίο* αν θέλετε σελίδες κεφαλίδας και χρειάζεται να στέλνετε ακολουθίες διαφυγής ή άλλες ακολουθίες αρχικοποίησης προκειμένου να τις εκτυπώσετε. (Αλλά είναι επίσης *μάταιο* αν θέλετε να χρεώνετε σελίδες κεφαλίδας στον λογαριασμό του αντίστοιχου χρήστη, από τη στιγμή που το LPD δεν στέλνει καμιά πληροφορία για τον χρήστη ή τον υπολογιστή

στο φίλτρο εξόδου.)

Το LPD επιτρέπει την συνύπαρξη ενός φίλτρου εξόδου και άλλων φίλτρων (κειμένου ή διαφορετικού τύπου) στον ίδιο εκτυπωτή. Σε αυτές τις περιπτώσεις, το LPD θα ξεκινά το φίλτρο εξόδου μόνο για την εκτύπωση της σελίδας κεφαλίδας (δείτε την ενότητα Σελίδες Κεφαλίδας). Το LPD θα αναμένει το φίλτρο εξόδου να *σταματήσει από μόνο του* όταν του στείλει δύο bytes: ένα ASCII 031 ακολουθούμενο από ένα ASCII 001. Όταν ένα φίλτρο εξόδου βλέπει αυτά τα δύο bytes (031, 001), θα πρέπει να σταματά στέλνοντας σήμα `SIGSTOP` στον εαυτό του. Όταν το LPD ολοκληρώσει την εκτέλεση και των υπολοίπων φίλτρων, θα επανεκκινήσει το φίλτρο εξόδου στέλνοντας του το σήμα `SIGCONT`.

Αν υπάρχει φίλτρο εξόδου, αλλά *δεν υπάρχει* φίλτρο κειμένου και το LPD δουλεύει σε εργασία απλού κειμένου, το LPD χρησιμοποιεί το φίλτρο εξόδου για την εκτέλεση της εργασίας. Όπως αναφέραμε και παραπάνω, το φίλτρο εξόδου θα εκτυπώσει κάθε αρχείο εργασίας στη σειρά, δίχως δυνατότητα παρεμβολής κενής σελίδας ή άλλων ρυθμίσεων στην τροφοδοσία χαρτιού, και πιθανώς αυτό να *μην* είναι επιθυμητό. Σχεδόν σε όλες τις περιπτώσεις, θα χρειαστείτε ένα φίλτρο κειμένου.

Το πρόγραμμα `lpf`, που αναφέραμε νωρίτερα σαν φίλτρο κειμένου, μπορεί να τρέξει και σαν φίλτρο εξόδου. Αν χρειάζεστε ένα γρήγορο φίλτρο εξόδου αλλά δεν θέλετε να γράψετε τον κώδικα ανίχνευσης των byte και τον κώδικα αποστολής σημάτων, δοκιμάστε το `lpf`. Μπορείτε επίσης να χρησιμοποιήσετε το `lpf` μέσα από ένα shell script το οποίο θα χειρίζεται τους κωδικούς αρχικοποίησης που ίσως να χρειάζεται ο εκτυπωτής.

16.4.1.6. `lpf`: ένα Φίλτρο Κειμένου

Το πρόγραμμα /usr/libexec/lpr/lpf που παρέχεται με τη διανομή εκτελέσιμων του FreeBSD είναι ένα φίλτρο κειμένου (φίλτρο εισόδου) που μπορεί να παραγραφοποιεί την έξοδο (εργασίες που έχουν σταλεί με `lpr -i`), να επιτρέπει την διέλευση literal χαρακτήρων (εργασίες που έχουν σταλεί με `lpr -l`), να ρυθμίζει την θέση εκτύπωσης με τη χρήση χαρακτήρων backspace και tab στην εργασία, και να κάνει καταμέτρηση των εκτυπωμένων σελίδων. Επίσης μπορεί να ενεργεί και σαν φίλτρο εξόδου.

Το `lpf` είναι κατάλληλο για διάφορα περιβάλλοντα εκτύπωσης. Αν και δεν έχει δυνατότητα αποστολής ακολουθιών αρχικοποίησης στον εκτυπωτή, είναι εύκολο να γράψετε ένα shell script για να κάνετε την απαραίτητη αρχικοποίηση και να εκτελέσετε έπειτα το `lpf`.

Για να κάνει σωστά καταμέτρηση σελίδων, το `lpf` χρειάζεται κατάλληλες τιμές για τις ικανότητες `pw` και `pl` στο αρχείο /etc/printcap. Χρησιμοποιεί αυτές τις τιμές για να προσδιορίσει πόσο κείμενο μπορεί να χωρέσει σε μία σελίδα και από πόσες σελίδες αποτελείται η εργασία του χρήστη. Για περισσότερες πληροφορίες σχετικά με την καταμέτρηση σελίδων, συμβουλευτείτε την Καταμέτρηση Χρήσης Εκτυπωτών.

16.4.2. Σελίδες Κεφαλίδας

Αν έχετε *αρκετούς* χρήστες, και όλοι τους χρησιμοποιούν διάφορους εκτυπωτές, τότε πιθανώς να θεωρείτε τις *σελίδες κεφαλίδας* ως αναγκαίο κακό.

Οι σελίδες κεφαλίδας, γνωστές επίσης και ως *banner* ή *σελίδες burst* αναγνωρίζουν σε ποιον ανήκουν οι εργασίες μετά την εκτύπωση τους. Συνήθως τυπώνονται με μεγάλα, έντονα γράμματα, και ίσως με διακοσμητικά περιγράμματα, ώστε σε μια στοίβα εκτυπώσεων να ξεχωρίζουν από τα

πραγματικά έγγραφα εργασιών των χρηστών. Επιτρέπουν έτσι στους χρήστες να βρίσκουν γρήγορα τις εργασίες τους. Το προφανές μειονέκτημα σε μια σελίδα κεφαλίδας είναι πως πρόκειται να εκτυπωθεί μια ακόμα σελίδα για κάθε μία εργασία. Η εφήμερη χρησιμότητα τους διαρκεί λίγα λεπτά, και ο προορισμός τους είναι ο κάδος αχρήστων/ανακύκλωσης. (Παρατηρήστε πως οι σελίδες κεφαλίδας είναι ανά εργασία, και όχι ανά αρχείο σε μια εργασία, επομένως το αχρηστευμένο χαρτί ίσως να μην είναι τόσο πολύ).

Το σύστημα LPD μπορεί να παρέχει αυτόματα σελίδες κεφαλίδας για τις εκτυπώσεις σας, *αν* ο εκτυπωτής σας μπορεί να εκτυπώσει άμεσα απλό κείμενο. Αν έχετε εκτυπωτή PostScript®, θα χρειαστείτε ένα εξωτερικό πρόγραμμα για να δημιουργήσετε την σελίδα κεφαλίδας. Δείτε το Σελίδες Κεφαλίδας σε Εκτυπωτές PostScript®.

16.4.2.1. Ενεργοποίηση Σελίδων Κεφαλίδας

Στην ενότητα Βασικές Ρυθμίσεις Εκτυπωτών, απενεργοποιήσαμε τις σελίδες κεφαλίδας με την καταχώριση `sh` (σημαίνει "suppress header") στο αρχείο /etc/printcap. Για να ενεργοποιήσετε τις σελίδες κεφαλίδας για κάποιον εκτυπωτή, απλά αφαιρέστε την ικανότητα `sh`.

Ακούγεται εύκολο, δεν νομίζετε;

Έτσι είναι. *Ίσως* χρειαστεί να παρέχετε ένα φίλτρο εξόδου για να στείλετε εντολές αρχικοποίησης στον εκτυπωτή. Εδώ είναι ένα παράδειγμα φίλτρου εξόδου για εκτυπωτές συμβατούς με τον τύπο PCL της Hewlett Packard:

```
#!/bin/sh
#
#  hpof - Output filter for Hewlett Packard PCL-compatible printers
#  Installed in /usr/local/libexec/hpof

printf "\033&k2G" || exit 2
exec /usr/libexec/lpr/lpf
```

Προσδιορίστε την διαδρομή προς το φίλτρο εξόδου στην ικανότητα `of`. Δείτε την ενότητα Φίλτρα Εξόδου για περισσότερες πληροφορίες.

Εδώ είναι ένα παράδειγμα αρχείου /etc/printcap για τον εκτυπωτή `teak` από το προηγούμενο παράδειγμα. Ενεργοποιήσαμε τις σελίδες κεφαλίδας και προσθέσαμε το παραπάνω φίλτρο εξόδου:

```
#
#  /etc/printcap for host orchid
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
        :if=/usr/local/libexec/hpif:\
        :vf=/usr/local/libexec/hpvf:\
        :of=/usr/local/libexec/hpof:
```

Τώρα, όταν οι χρήστες εκτυπώνουν εργασίες στον `teak`, θα παίρνουν και μία σελίδα κεφαλίδας ανά

εργασία. Αν οι χρήστες θέλουν να ξοδεύουν χρόνο ψάχνοντας για τις εκτυπώσεις τους, μπορούν να παρεμποδίσουν τις σελίδες κεφαλίδας αποστέλλοντας τις εργασίες τους με `lpr -h`. Δείτε την ενότητα Επιλογές Σελίδων Κεφαλίδας για περισσότερες επιλογές του lpr(1).

Το LPD στέλνει το χαρακτήρα αλλαγής σελίδας (form feed) αμέσως μετά τη σελίδα κεφαλίδας. Αν ο εκτυπωτής σας χρησιμοποιεί διαφορετικό χαρακτήρα ή ακολουθία χαρακτήρων για την αλλαγή σελίδας, προσδιορίστε τα με την ικανότητα `ff` στο αρχείο /etc/printcap.

16.4.2.2. Έλεγχος Σελίδων Κεφαλίδας

Μετά την ενεργοποίηση των σελίδων κεφαλίδας, το LPD θα παράγει μία *επιμήκη κεφαλίδα*, μία ολόκληρη σελίδα με μεγάλα γράμματα που προσδιορίζει τον χρήστη, τον υπολογιστή (host), και την εργασία. Εδώ είναι ένα παράδειγμα (η `kelly` εκτύπωσε την εργασία με όνομα "outline" από τον υπολογιστή `rose`):

```
k                 ll       ll
k                  l        l
k                  l        l
k   k     eeee     l        l     y    y
k  k     e    e    l        l     y    y
k k      eeeeee    l        l     y    y
kk k     e         l        l     y    y
k   k    e    e    l        l     y   yy
k    k    eeee    lll      lll     yyy y
                                      y
                                     y    y
                                      yyyy

                           ll
                  t         l        i
                  t         l
 oooo    u    u   ttttt     l       ii     n nnn     eeee
o    o   u    u     t       l        i     nn   n   e    e
o    o   u    u     t       l        i     n    n   eeeeee
o    o   u    u     t       l        i     n    n   e
o    o   u   uu     t  t     l        i     n    n   e    e
 oooo     uuu u      tt     lll      iii    n    n    eeee

r rrr     oooo     ssss     eeee
rr   r   o    o   s    s   e    e
r        o    o    ss      eeeeee
r        o    o      ss    e
r        o    o   s    s   e    e
r         oooo     ssss     eeee

                                    Job:  outline
                                    Date: Sun Sep 17 11:04:58 1995
```

Το LPD προσθέτει μια εντολή αλλαγής σελίδας (form feed) μετά από αυτό το κείμενο έτσι ώστε η εργασία να ξεκινήσει σε νέα σελίδα (εκτός αν έχετε προσδιορίσει την ικανότητα `sf` (suppress form feeds) για τον εκτυπωτή στο αρχείο /etc/printcap).

Αν προτιμάτε, το LPD μπορεί να φτιάξει μια *μικρότερου μήκους κεφαλίδα*. Προσδιορίστε `sb` (short banner) στο αρχείο /etc/printcap. Η σελίδα κεφαλίδας θα μοιάζει σαν αυτή:

```
rose:kelly  Job: outline  Date: Sun Sep 17 11:07:51 1995
```

Το LPD τυπώνει (από προεπιλογή) πρώτα την σελίδα κεφαλίδας, και μετά την εργασία. Για να αντιστρέψετε την σειρά, χρησιμοποιήστε την ικανότητα `hl` (header last) στο αρχείο /etc/printcap.

16.4.2.3. Καταμέτρηση με Σελίδες Κεφαλίδας

Η χρήση των προεγκατεστημένων σελίδων κεφαλίδας του LPD ουσιαστικά υποχρεώνουν την τήρηση του παρακάτω κανόνα όταν κάνουμε καταμέτρηση χρήσης του εκτυπωτή: Οι σελίδες κεφαλίδας πρέπει να διατίθενται *ελεύθερα (δίχως χρέωση)*.

Γιατί;

Διότι το φίλτρο εξόδου είναι το μοναδικό εξωτερικό πρόγραμμα που έχει τον έλεγχο στην εκτύπωση της κεφαλίδας και θα μπορούσε να κάνει καταμέτρηση, αλλά ωστόσο δεν παρέχει καμία πληροφορία για *τον χρήστη ή τον υπολογιστή* ή κάποιο άλλο αρχείο καταμέτρησης, επομένως δεν γνωρίζει σε ποιόν να αποδώσει την χρήση του εκτυπωτή. Δεν αρκεί απλά να "προσθέσετε μία ακόμη σελίδα στην καταμέτρηση" τροποποιώντας το φίλτρο κειμένου ή οποιοδήποτε άλλο φίλτρο μετατροπής (το οποίο διαθέτει τις πληροφορίες χρήστη και υπολογιστή), από τη στιγμή που οι χρήστες έχουν την δυνατότητα να παρεμποδίσουν τις σελίδες κεφαλίδας με `lpr -h`. Θα μπορούσαν πάλι να χρεωθούν για σελίδες κεφαλίδας που δεν εκτύπωσαν. Βασικά, η `lpr -h` θα είναι η προτιμώμενη επιλογή σε ένα περιβάλλον που οι χρήστες έχουν οικολογική συνείδηση, αλλά δεν μπορείτε πραγματικά να παροτρύνετε οποιονδήποτε να τη χρησιμοποιήσει.

Δεν είναι αρκετό απλά κάθε φίλτρο σας να δημιουργεί τη δικιά του σελίδα κεφαλίδας (έτσι ώστε να μπορεί να χρεώνει με αυτό τον τρόπο). Αν οι χρήστες επιθυμούν την επιλογή παρεμπόδισης των σελίδων κεφαλίδας με `lpr -h`, θα συνεχίσουν να τις παραλαμβάνουν - και να χρεώνονται για αυτές - αφού το LPD δεν έχει δυνατότητα να περάσει σε οποιοδήποτε φίλτρο την επιλογή `-h`.

Επομένως, ποιες επιλογές έχετε;

Μπορείτε:

- Να αποδεχθείτε την υπόδειξη του LPD και να παρέχετε τις σελίδες κεφαλίδας ελεύθερα.
- Να εγκαταστήσετε εναλλακτικές λύσεις αντί του LPD, όπως το LPRng. Η ενότητα Εναλλακτικές Λύσεις για τον Στάνταρ Spooler δίνει περισσότερες πληροφορίες για άλλες εφαρμογές παροχέτευσης που μπορείτε να χρησιμοποιήσετε αντί για το LPD.
- Να γράψετε ένα *έξυπνο* φίλτρο εξόδου. Υπό κανονικές συνθήκες, ένα "φίλτρο εξόδου" δεν κάνει τίποτε παραπάνω από την αρχικοποίηση ενός εκτυπωτή ή μερικές απλές μετατροπές χαρακτήρων. Είναι κατάλληλο για σελίδες κεφαλίδας και για εργασίες απλού κειμένου (όταν δεν υπάρχει φίλτρο (εισόδου) κειμένου). Αλλά αν υπάρχει φίλτρο κειμένου για εργασίες απλού

κειμένου, τότε το LPD θα ενεργοποιεί το φίλτρο εξόδου μόνο για τις σελίδες κεφαλίδας. Και το φίλτρο εξόδου μπορεί να αναλύει το κείμενο της σελίδας κεφαλίδας που δημιουργεί το LPD για να προσδιορίζει τον χρήστη και τον υπολογιστή, ώστε να χρεώνει τις σελίδες κεφαλίδας. Το μόνο επιπλέον πρόβλημα με αυτή τη μέθοδο είναι πως το φίλτρο εξόδου εξακολουθεί να μη γνωρίζει ποιό αρχείο καταμέτρησης να χρησιμοποιήσει (δεν του έχει δοθεί το όνομα του αρχείου από την ικανότητα `af`), αλλά αν το όνομα του αρχείου σας είναι γνωστό, μπορείτε να το ενσωματώσετε απευθείας στον κώδικα του φίλτρου εξόδου. Για να διευκολύνετε την διαδικασία ανάλυσης, χρησιμοποιήστε την ικανότητα `sh` (short header) στο /etc/printcap. Ίσως πάλι όλα αυτά να είναι υπερβολικά κοπιαστικά, ενώ είναι σίγουρο πως οι χρήστες θα εκτιμήσουν τον γενναιόδωρο διαχειριστή συστήματος που επιτρέπει ελεύθερα τις σελίδες κεφαλίδας.

16.4.2.4. Σελίδες Κεφαλίδας σε Εκτυπωτές PostScript®

Όπως περιγράψαμε παραπάνω, το LPD μπορεί να δημιουργήσει μία σελίδα κεφαλίδας απλού κειμένου, κατάλληλη για πολλούς εκτυπωτές. Οι εκτυπωτές PostScript®, φυσικά, δεν μπορούν να τυπώσουν κατευθείαν απλό κείμενο, επομένως αυτή η δυνατότητα του LPD για τις σελίδες κεφαλίδας είναι άχρηστη σε αυτή την περίπτωση.

Ένας προφανής τρόπος να παρέχονται σελίδες κεφαλίδας είναι να δημιουργούνται από κάθε φίλτρο μετατροπής και το φίλτρο κειμένου. Τα φίλτρα θα πρέπει να δέχονται ως παραμέτρους το όνομα του χρήστη και του υπολογιστή ώστε να δημιουργούν την κατάλληλη σελίδα κεφαλίδας. Το μειονέκτημα αυτής της μεθόδου είναι πως οι χρήστες θα εκτυπώνουν πάντα σελίδα κεφαλίδας, ακόμη κι αν αποστέλλουν την εργασία τους με `lpr -h`.

Επιτρέψτε μας να εξερευνήσουμε αυτή τη μέθοδο. Το ακόλουθο script δέχεται τρεις παραμέτρους (το όνομα χρήστη - login name, το όνομα του υπολογιστή - host name, και το όνομα εργασίας) και δημιουργεί μία απλή σελίδα κεφαλίδας PostScript®:

```
#!/bin/sh
#
#  make-ps-header - make a PostScript header page on stdout
#  Installed in /usr/local/libexec/make-ps-header
#

#
#  These are PostScript units (72 to the inch).  Modify for A4 or
#  whatever size paper you are using:
#
page_width=612
page_height=792
border=72

#
#  Check arguments
#
if [ $# -ne 3 ]; then
    echo "Usage: `basename $0` <user> <host> <job>" 1>&2
    exit 1
fi
```

```
#
#  Save these, mostly for readability in the PostScript, below.
#
user=$1
host=$2
job=$3
date=`date`

#
#  Send the PostScript code to stdout.
#
exec cat <<EOF
%!PS

%
%  Make sure we do not interfere with user's job that will follow
%
save

%
%  Make a thick, unpleasant border around the edge of the paper.
%
$border $border moveto
$page_width $border 2 mul sub 0 rlineto
0 $page_height $border 2 mul sub rlineto
currentscreen 3 -1 roll pop 100 3 1 roll setscreen
$border 2 mul $page_width sub 0 rlineto closepath
0.8 setgray 10 setlinewidth stroke 0 setgray

%
%  Display user's login name, nice and large and prominent
%
/Helvetica-Bold findfont 64 scalefont setfont
$page_width ($user) stringwidth pop sub 2 div $page_height 200 sub moveto
($user) show

%
%  Now show the boring particulars
%
/Helvetica findfont 14 scalefont setfont
/y 200 def
[ (Job:) (Host:) (Date:) ] {
200 y moveto show /y y 18 sub def }
forall

/Helvetica-Bold findfont 14 scalefont setfont
/y 200 def
[ ($job) ($host) ($date) ] {
        270 y moveto show /y y 18 sub def
} forall
```

```
%
% That is it
%
restore
showpage
EOF
```

Τώρα, καθένα από τα φίλτρα μετατροπής και το φίλτρο κειμένου μπορούν να καλέσουν το script, πρώτα για να δημιουργήσουν τη σελίδα κεφαλίδας, και έπειτα για να εκτυπώσουν την εργασία του χρήστη. Ακολουθεί το φίλτρο μετατροπής DVI που δείξαμε νωρίτερα, ειδικά διαμορφωμένο για να φτιάξουμε μια σελίδα κεφαλίδας:

```
#!/bin/sh
#
#  psdf - DVI to PostScript printer filter
#  Installed in /usr/local/libexec/psdf
#
#  Invoked by lpd when user runs lpr -d
#

orig_args="$@"

fail() {
    echo "$@" 1>&2
    exit 2
}

while getopts "x:y:n:h:" option; do
    case $option in
        x|y)  ;; # Ignore
        n)    login=$OPTARG ;;
        h)    host=$OPTARG ;;
        *)    echo "LPD started `basename $0` wrong." 1>&2
              exit 2
              ;;
    esac
done

[ "$login" ] || fail "No login name"
[ "$host" ] || fail "No host name"

( /usr/local/libexec/make-ps-header $login $host "DVI File"
  /usr/local/bin/dvips -f ) | eval /usr/local/libexec/lprps $orig_args
```

Παρατηρήστε πως το φίλτρο πρέπει να αναλύσει την λίστα παραμέτρων για να προσδιορίσει το όνομα χρήστη και υπολογιστή. Η μέθοδος ανάλυσης είναι παρόμοια και για τα υπόλοιπα φίλτρα μετατροπής. Το φίλτρο κειμένου παίρνει ένα ελαφρώς διαφορετικό σετ παραμέτρων, (δείτε την ενότητα Πως δουλεύουν τα Φίλτρα).

Όπως αναφέραμε προηγούμενα, ο παραπάνω σχεδιασμός, αν και πραγματικά απλός, απενεργοποιεί την επιλογή "παρεμπόδισης σελίδων κεφαλίδας" (την επιλογή `-h`) του `lpr`. Αν οι χρήστες επιθυμούν να σώσουν ένα δέντρο (ή λίγα χρήματα, αν χρεώνετε τις σελίδες κεφαλίδας), δεν θα υπάρχει τρόπος για να γίνει αυτό, από τη στιγμή που κάθε εκτύπωση μέσω των φίλτρων θα συνοδεύεται και από μια σελίδα κεφαλίδας για κάθε εργασία.

Για να επιτρέψετε στους χρήστες να απενεργοποιούν τις σελίδες κεφαλίδας ανά εργασία, θα πρέπει να χρησιμοποιήσετε το τέχνασμα που παρουσιάσαμε στην ενότητα Καταμέτρηση με Σελίδες Κεφαλίδας: δηλαδή να γράψετε ένα φίλτρο εξόδου που να αναλύει την σελίδα κεφαλίδας που δημιουργείται από το LPD και να κατασκευάζει μια PostScript® έκδοση. Αν ο χρήστης στείλει μια εργασία με `lpr -h`, τότε ούτε το LPD, ούτε το φίλτρο εξόδου θα φτιάξουν σελίδα κεφαλίδας. Σε όλες τις άλλες περιπτώσεις, το φίλτρο εξόδου θα διαβάζει το κείμενο από το LPD και θα στέλνει τον κατάλληλο κώδικα PostScript® στον εκτυπωτή ώστε να εκτυπώνεται η σελίδα κεφαλίδας.

Αν έχετε εκτυπωτή PostScript® με σειριακή σύνδεση, μπορείτε να κάνετε χρήση της `lprps`, η οποία συνοδεύεται από ένα φίλτρο εξόδου, το `psof`, το οποία κάνει τα παραπάνω. Σημειώστε πως το `psof` δεν χρεώνει για τις σελίδες κεφαλίδας.

16.4.3. Εκτυπώσεις μέσω Δικτύου

Το FreeBSD υποστηρίζει τις εκτυπώσεις μέσω δικτύου: μπορεί να στείλει εργασίες σε απομακρυσμένους εκτυπωτές. Η έννοια της δικτυακής εκτύπωσης αναφέρεται γενικά σε δύο διαφορετικά πράγματα:

- Πρόσβαση σε εκτυπωτή συνδεδεμένο σε απομακρυσμένο υπολογιστή (host). Εγκαθιστάτε έναν εκτυπωτή με συμβατική σειριακή ή παράλληλη σύνδεση σε ένα υπολογιστή. Έπειτα, ρυθμίζετε το LPD για να ενεργοποιηθεί η πρόσβαση στον εκτυπωτή από άλλους υπολογιστές του δικτύου. Η ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές εξηγεί τις απαραίτητες ενέργειες.
- Πρόσβαση σε εκτυπωτή συνδεδεμένο κατευθείαν στο δίκτυο. Εκτός (ή αντί) της συμβατικής σειριακής ή παράλληλης θύρας, ο εκτυπωτής πρέπει να έχει επιπρόσθετα μια δικτυακή διασύνδεση. Ένας τέτοιος εκτυπωτής δουλεύει ως εξής:
  - Μπορεί να καταλαβαίνει το πρωτόκολλο LPD και να δημιουργεί ουρά αναμονής για τις εργασίες που προέρχονται από απομακρυσμένους υπολογιστές. Σε αυτή την περίπτωση, ενεργεί σαν ένας κανονικός υπολογιστής που εκτελεί το LPD. Ακολουθήστε την ίδια διαδικασία με την ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές για να εγκαταστήσετε αυτόν τον εκτυπωτή.
  - Μπορεί να υποστηρίζει σύνδεση δικτυακής ροής δεδομένων (data stream). Σε αυτή την περίπτωση, "συνδέετε" τον εκτυπωτή σε έναν υπολογιστή συνδεδεμένο στο δίκτυο, ο οποίος θα είναι υπεύθυνος για την παροχέτευση των εργασιών και την αποστολή τους στον εκτυπωτή. Η ενότητα Εκτυπωτές Με Συνδέσεις Δικτύου δίνει μερικές συμβουλές για την εγκατάσταση εκτυπωτών αυτού του τύπου.

16.4.3.1. Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές

Το σύστημα παροχέτευσης LPD έχει ενσωματωμένη υποστήριξη για την αποστολή εργασιών σε άλλους υπολογιστές που εκτελούν το LPD (ή που είναι συμβατοί με το LPD). Αυτό το χαρακτηριστικό σας επιτρέπει να εγκαταστήσετε έναν εκτυπωτή σε ένα υπολογιστή και να έχετε

πρόσβαση σε αυτόν από άλλους. Επίσης δουλεύει και με εκτυπωτές που έχουν δικτυακές διασυνδέσεις που καταλαβαίνουν το πρωτόκολλο LPD.

Για να ενεργοποιήσετε αυτόν τον τύπο απομακρυσμένης εκτύπωσης, εγκαταστήστε πρώτα έναν εκτυπωτή σε ένα υπολογιστή, τον *υπολογιστή εκτύπωσης (printer host)*, χρησιμοποιώντας την απλή εγκατάσταση εκτυπωτή που περιγράφεται στην ενότητα Βασικές Ρυθμίσεις Εκτυπωτών. Κάντε όσες προχωρημένες ρυθμίσεις χρειάζεστε όπως αναφέρεται στις Ρυθμίσεις Εκτυπωτών για Προχωρημένους. Ελέγξτε τον εκτυπωτή και δείτε αν δουλεύει με τα χαρακτηριστικά του LPD που έχετε ενεργοποιήσει. Επίσης βεβαιωθείτε πως ο *τοπικός υπολογιστής (local host)* είναι εξουσιοδοτημένος να χρησιμοποιεί τις υπηρεσίες του LPD στον *απομακρυσμένο υπολογιστή (remote host)* (δείτε Παρεμπόδιση Εργασιών από Απομακρυσμένους Υπολογιστές).

Εάν χρησιμοποιείτε εκτυπωτή με δικτυακή διασύνδεση που είναι συμβατός με το LPD, τότε ο *ο υπολογιστής εκτύπωσης (printer host)* είναι ο εν λόγω εκτυπωτής, και το *όνομα του εκτυπωτή* είναι το όνομα που έχετε ορίσει για τον εκτυπωτή. Δείτε την τεκμηρίωση που συνοδεύει τον εκτυπωτή σας και/ή την κάρτα δικτύου του.

Αν χρησιμοποιείτε Hewlett Packard Laserjet με όνομα εκτυπωτή `text` θα γίνονται αυτόματα οι μετατροπές από LF σε CRLF, επομένως δεν χρειάζεται να τρέξετε το script hpif.

Επομένως, στους υπόλοιπους υπολογιστές όπου επιθυμείτε να έχετε πρόσβαση στον εκτυπωτή, απλά κάντε μια καταχώριση στο αρχείο /etc/printcap με τα ακόλουθα στοιχεία:

1. Ονομάστε την καταχώριση όπως επιθυμείτε: Για δική σας ευκολία πιθανώς να θέλετε να χρησιμοποιήσετε το ίδιο όνομα και τα ίδια παρωνύμια με αυτά του υπολογιστή εκτύπωσης.
2. Αφήστε την ικανότητα `lp` κενή, για την ακρίβεια (`:lp=:`).
3. Δημιουργήστε ένα κατάλογο spooling και προσδιορίστε την τοποθεσία του με την ικανότητα `sd`. Το LPD θα αποθηκεύει εδώ τις εργασίες πριν την αποστολή τους στον υπολογιστή εκτύπωσης.
4. Τοποθετήστε το όνομα του υπολογιστή εκτύπωσης στην ικανότητα `rm`.
5. Τοποθετήστε το όνομα του εκτυπωτή στην ικανότητα `rp`, στον *υπολογιστή εκτύπωσης*.

Αυτό είναι όλο. Δεν χρειάζεται να δημιουργήσετε λίστα φίλτρων μετατροπής, διαστάσεις σελίδας, ή οτιδήποτε άλλο στο αρχείο /etc/printcap.

Εδώ είναι ένα παράδειγμα. Ο υπολογιστής `rose` έχει δύο εκτυπωτές, τον `bamboo` και τον `rattan`. Θέλουμε να ενεργοποιήσουμε τις εκτυπώσεις σε αυτούς τους εκτυπωτές για τους χρήστες του απομακρυσμένου υπολογιστή `orchid`. Εδώ είναι το αρχείο /etc/printcap του υπολογιστή `orchid` (δείτε πιο πίσω στην ενότητα Ενεργοποίηση Σελίδων Κεφαλίδας). Ήδη έχει μια καταχώριση για τον εκτυπωτή `teak`. Εδώ προσθέσαμε τις απαραίτητες καταχωρίσεις για τους δύο εκτυπωτές του υπολογιστή `rose`:

```
#
#  /etc/printcap for host orchid - added (remote) printers on rose
#

#
```

```
#  teak is local; it is connected directly to orchid:
#
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:\
        :if=/usr/local/libexec/ifhp:\
        :vf=/usr/local/libexec/vfhp:\
        :of=/usr/local/libexec/ofhp:

#
#  rattan is connected to rose; send jobs for rattan to rose:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

#
#  bamboo is connected to rose as well:
#
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:
```

Το μόνο που απομένει είναι να δημιουργήσουμε τους καταλόγους spooling στον κόμβο `orchid`:

```
# mkdir -p /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chmod 770 /var/spool/lpd/rattan /var/spool/lpd/bamboo
# chown daemon:daemon /var/spool/lpd/rattan /var/spool/lpd/bamboo
```

Τώρα, οι χρήστες του `orchid` μπορούν να εκτυπώνουν στον `rattan` και στον `bamboo`. Αν, για παράδειγμα, ένας χρήστης του `orchid` πληκτρολογήσει:

```
% lpr -P bamboo -d sushi-review.dvi
```

το σύστημα LPD στον `orchid` θα αντιγράψει την εργασία στον κατάλογο spooling /var/spool/lpd/bamboo και θα σημειώσει πως πρόκειται για εργασία DVI. Μόλις ο υπολογιστής `rose` έχει διαθέσιμο χώρο στον κατάλογο spooling του `bamboo`, τα δύο LPDs θα μεταφέρουν το αρχείο στον `rose`. Το αρχείο θα μπει σε ουρά αναμονής στον υπολογιστή `rose` έως ότου εκτυπωθεί. Θα μετατραπεί από DVI σε PostScript® (αφού ο `bamboo` είναι εκτυπωτής PostScript®) στον υπολογιστή `rose`.

16.4.3.2. Εκτυπωτές με Συνδέσεις Δικτύου

Συχνά, όταν αγοράζετε κάρτα δικτύου για εκτυπωτή, έχετε τη δυνατότητα επιλογής δύο εκδόσεων: η μία είναι προσομοίωση του spooler (η πιο ακριβή έκδοση) ενώ η άλλη απλά σας επιτρέπει να στέλνετε δεδομένα μέσω αυτής σαν να χρησιμοποιούσατε μια σειριακή ή παράλληλη θύρα (η φτηνή έκδοση). Αυτή η ενότητα περιγράφει πως να χρησιμοποιείτε την φτηνή έκδοση. Για την πιο ακριβή έκδοση μπορείτε να βρείτε περισσότερες πληροφορίες στην προηγούμενη ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές.

Η μορφή του αρχείου /etc/printcap σας επιτρέπει να ορίσετε τη διασύνδεση - σειριακή ή παράλληλη

- που θα χρησιμοποιήσετε, και (αν χρησιμοποιείτε σειριακή διασύνδεση) τον ρυθμό baud, πιθανούς ελέγχους ροής, καθυστερήσεις για tabs, μετατροπές για χαρακτήρες νέας γραμμής, και άλλα. Αλλά δεν υπάρχει τρόπος να ορίσετε μια σύνδεση σε εκτυπωτή που ακούει σε θύρα TCP/IP ή άλλο τύπο δικτύου.

Για να στείλετε δεδομένα σε ένα δικτυακό εκτυπωτή, χρειάζεται να αναπτύξετε προγράμματα επικοινωνίας που να καλούνται από φίλτρα κειμένου και φίλτρα μετατροπής. Εδώ έχουμε ένα τέτοιο παράδειγμα: το script `netprint` παίρνει όλα τα δεδομένα από το standard input και τα στέλνει σε έναν εκτυπωτή συνδεδεμένο στο δίκτυο. Ορίζουμε στο `netprint` το όνομα του εκτυπωτή ως πρώτη παράμετρο, και τον αριθμό θύρας στην οποία συνδέεται ως δεύτερη. Σημειώστε πως αυτός ο τρόπος υποστηρίζει μόνο επικοινωνία μιας κατεύθυνσης (από το FreeBSD στον εκτυπωτή). Πολλοί δικτυακοί εκτυπωτές υποστηρίζουν αμφίδρομη επικοινωνία, και είναι πολύ πιθανό να επιθυμείτε να εκμεταλλευτείτε τα προτερήματα τους (για να ελέγχετε την κατάσταση του εκτυπωτή, για καταμέτρηση εκτυπώσεων, κλπ.).

```
#!/usr/bin/perl
#
#  netprint - Text filter for printer attached to network
#  Installed in /usr/local/libexec/netprint
#
$#ARGV eq 1 || die "Usage: $0 <printer-hostname> <port-number>";

$printer_host = $ARGV[0];
$printer_port = $ARGV[1];

require 'sys/socket.ph';

($ignore, $ignore, $protocol) = getprotobyname('tcp');
($ignore, $ignore, $ignore, $ignore, $address)
    = gethostbyname($printer_host);

$sockaddr = pack('S n a4 x8', &AF_INET, $printer_port, $address);

socket(PRINTER, &PF_INET, &SOCK_STREAM, $protocol)
    || die "Can't create TCP/IP stream socket: $!";
connect(PRINTER, $sockaddr) || die "Can't contact $printer_host: $!";
while (<STDIN>) { print PRINTER; }
exit 0;
```

Μπορείτε να χρησιμοποιήσετε αυτό το script σε διάφορα φίλτρα. Ας υποθέσουμε πως έχουμε έναν εκτυπωτή γραμμής Diablo 750-N συνδεδεμένο στο δίκτυο. Ο εκτυπωτής δέχεται δεδομένα προς εκτύπωση στην θύρα 5100. Το όνομα του εκτυπωτή στο δίκτυο είναι `scrivener`. Εδώ είναι το φίλτρο κειμένου για τον εκτυπωτή:

```
#!/bin/sh
#
#  diablo-if-net - Text filter for Diablo printer `scrivener' listening
#  on port 5100.   Installed in /usr/local/libexec/diablo-if-net
```

```
#
exec /usr/libexec/lpr/lpf "$@" | /usr/local/libexec/netprint scrivener 5100
```

16.4.4. Έλεγχος Πρόσβασης και Περιορισμοί στη Χρήση των Εκτυπωτών

Αυτή η ενότητα δίνει πληροφορίες για τον έλεγχο πρόσβασης και τον περιορισμό χρήσης των εκτυπωτών. Το σύστημα LPD σας επιτρέπει να ελέγχετε ποιός μπορεί να έχει πρόσβαση σε κάθε εκτυπωτή, τόσο τοπικά όσο και απομακρυσμένα, και επίσης αν μπορούν οι χρήστες να εκτυπώνουν πολλαπλά αντίγραφα, πόσο μεγάλες μπορούν να είναι οι εργασίες τους, και πόσο μεγάλες μπορούν να γίνουν οι ουρές αναμονής (print queues).

16.4.4.1. Περιορισμός Εκτύπωσης Πολλαπλών Αντιγράφων

Το σύστημα LPD διευκολύνει τους χρήστες να εκτυπώσουν πολλαπλά αντίγραφα ενός αρχείου. Οι χρήστες μπορούν να εκτυπώνουν εργασίες με `lpr -#5` (για παράδειγμα) και να παίρνουν πέντε αντίγραφα κάθε αρχείου της εργασίας εκτύπωσης. Το αν αυτό είναι καλό, εξαρτάται από εσάς.

Αν πιστεύετε πως τα πολλαπλά αντίγραφα δημιουργούν άσκοπη καταπόνηση των εκτυπωτών σας, μπορείτε να απενεργοποιήσετε την επιλογή `-` στο `lpr(1)` προσθέτοντας την ικανότητα `sc` στο αρχείο `/etc/printcap`. Όταν οι χρήστες αποστέλλουν εργασίες με την επιλογή `-`, θα βλέπουν:

```
lpr: multiple copies are not allowed
```

Σημειώστε πως αν έχετε ρυθμίσει πρόσβαση σε έναν εκτυπωτή απομακρυσμένα (δείτε την ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές), θα χρειαστεί να προσθέσετε την ικανότητα `sc` σε όλα τα απομακρυσμένα αρχεία /etc/printcap, διαφορετικά οι χρήστες θα έχουν ακόμη την δυνατότητα να αποστέλλουν εργασίες πολλαπλών αντιγράφων χρησιμοποιώντας διαφορετικό κόμβο.

Εδώ είναι ένα παράδειγμα. Αυτό είναι το αρχείο /etc/printcap για τον κόμβο `rose`. Ο εκτυπωτής `rattan` είναι δυνατό μηχάνημα και επιτρέπει την εκτύπωση πολλαπλών αντιγράφων, αλλά ο εκτυπωτής laser `bamboo` είναι πιο ευαίσθητο, επομένως θα απενεργοποιήσουμε τη δυνατότητα πολλαπλών αντιγράφων προσθέτοντας την ικανότητα `sc`:

```
#
#  /etc/printcap for host rose - restrict multiple copies on bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Τώρα, θα χρειαστεί να προσθέσουμε επίσης την ικανότητα sc στο αρχείο /etc/printcap του κόμβου orchid (και ενώ βρισκόμαστε σε αυτό, επιτρέψτε μας να απενεργοποιήσουμε τα πολλαπλά αντίγραφα για τον εκτυπωτή teak):

```
#
#  /etc/printcap for host orchid - no multiple copies for local
#  printer teak or remote printer bamboo
teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
        :lp=/dev/lpt0:sd=/var/spool/lpd/teak:mx#0:sc:\
        :if=/usr/local/libexec/ifhp:\
        :vf=/usr/local/libexec/vfhp:\
        :of=/usr/local/libexec/ofhp:

rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :lp=:rm=rose:rp=rattan:sd=/var/spool/lpd/rattan:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :lp=:rm=rose:rp=bamboo:sd=/var/spool/lpd/bamboo:sc:
```

Χρησιμοποιώντας την ικανότητα sc, προλαμβάνουμε την χρήση των εντολών lpr -#, αλλά δεν έχουμε ακόμη την δυνατότητα να παρεμποδίσουμε τους χρήστες να τρέξουν την εντολή lpr(1) πολλές φορές, ή να αποστείλουν το ίδιο αρχείο πολλές φορές σε μία μοναδική εργασία, όπως εδώ:

```
% lpr forsale.sign forsale.sign forsale.sign forsale.sign forsale.sign
```

Υπάρχουν πολλοί τρόποι πρόληψης αυτών των ενεργειών (συμπεριλαμβάνοντας και την περίπτωση να το αγνοήσετε) που είστε ελεύθεροι να εξερευνήσετε.

16.4.4.2. Περιορίζοντας την Πρόσβαση σε Εκτυπωτές

Μπορείτε να ελέγχετε ποιός μπορεί να εκτυπώνει σε ποιόν εκτυπωτή χρησιμοποιώντας τους μηχανισμούς ομάδων (groups) του UNIX® και την ικανότητα rg στο /etc/printcap. Απλά τοποθετήστε τους χρήστες που θέλετε να έχουν πρόσβαση σε κάποιον εκτυπωτή σε μια συγκεκριμένη ομάδα (χρηστών), και δηλώστε αυτή την ομάδα στην ικανότητα rg.

Όλοι οι χρήστες που δεν ανήκουν στην ομάδα (συμπεριλαμβανομένου και του root) θα δέχονται το ακόλουθο μήνυμα: lpr: Not a member of the restricted group όταν προσπαθούν να εκτυπώσουν στον ελεγχόμενο εκτυπωτή.

Όπως και με την ικανότητα sc (περιορισμού πολλαπλών αντιγράφων), θα χρειαστεί να προσδιορίσετε την rg στους απομακρυσμένους κόμβους που θα έχουν πρόσβαση στους εκτυπωτές σας, αν νομίζετε πως αυτό είναι σωστό (δείτε την ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές).

Για παράδειγμα, θα αφήσουμε για όλους ελεύθερη την πρόσβαση στον εκτυπωτή rattan, αλλά μόνο οι χρήστες της ομάδας artists θα μπορούν να χρησιμοποιήσουν τον bamboo. Εδώ είναι το γνωστό μας /etc/printcap για τον κόμβο rose:

```
#
#  /etc/printcap for host rose - restricted group for bamboo
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Επιτρέψτε μας να μην αλλάξουμε το αρχείο /etc/printcap από το άλλο παράδειγμα (για τον υπολογιστή `orchid`). Φυσικά, οποιοσδήποτε χρήστης του `orchid` μπορεί να εκτυπώσει στον `bamboo`. Ίσως όμως να επιτρέπουμε μόνον σε συγκεκριμένους χρήστες την πρόσβαση στον υπολογιστή `orchid`, και θέλουμε αυτοί οι χρήστες να έχουν πρόσβαση στον εκτυπωτή. Ή ίσως πάλι, και όχι.

Επιτρέπεται μόνο μια περιορισμένη ομάδα ανά εκτυπωτή.

16.4.4.3. Έλεγχος Μεγέθους των Απεσταλμένων Εργασιών

Αν πολλοί χρήστες έχουν πρόσβαση στους εκτυπωτές σας, πιθανώς να χρειάζεται να θέσετε ένα ανώτατο όριο στο επιτρεπόμενο μέγεθος αρχείων που μπορούν να αποστείλουν οι χρήστες για εκτύπωση. Ακόμα και αν υπάρχει αρκετός χώρος στο σύστημα αρχείων που φιλοξενεί τους καταλόγους spool, θα πρέπει ωστόσο να βεβαιωθείτε ότι επαρκεί για τις εργασίες όλων των χρηστών.

Το LPD σας επιτρέπει να οριοθετήσετε το μέγιστο αριθμό bytes που περιέχει μια εργασία, με την ικανότητα `mx`. Η μονάδα μέτρησης είναι σε `BUFSIZ` blocks, τα οποία είναι 1024 bytes. Αν θέσετε μηδέν σε αυτή την ικανότητα, δεν θα υπάρχουν όρια στο μέγεθος των αρχείων. Ωστόσο, αν δεν έχει οριστεί η ικανότητα `mx`, τότε θα χρησιμοποιείται η προεπιλεγμένη τιμή των 1000 blocks.

Το όριο εφαρμόζεται στα *αρχεία* μιας εργασίας, και *όχι* στο συνολικό μέγεθος της εργασίας.

Το LPD δεν θα απορρίψει ένα αρχείο που ξεπερνά το όριο μεγέθους που έχετε θέσει. Αντιθέτως, θα το τοποθετήσει στην ουρά αναμονής με μέγεθος ίσο με το μέγιστο επιτρεπτό, το οποίο και θα εκτυπώσει τελικά. Το υπόλοιπο αρχείο απορρίπτεται. Αν αυτός είναι σωστός ή λανθασμένος τρόπος αντιμετώπισης για την υπέρβαση του ορίου, είναι θέμα προς συζήτηση.

Ας οριοθετήσουμε στο παράδειγμα μας τους εκτυπωτές `rattan` και `bamboo`. Επειδή τα αρχεία PostScript® των `artists` τείνουν προς μεγάλα μεγέθη, θα θέσουμε ένα όριο πέντε megabytes. Δεν θα θέσουμε όρια για τον εκτυπωτή γραμμής απλού κειμένου:

```
#
#  /etc/printcap for host rose
```

```
#

#
#  No limit on job size:
#
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:mx#0:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:

#
#  Limit of five megabytes:
#
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:rw:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Και πάλι, τα όρια εφαρμόζονται μόνο για τους τοπικούς χρήστες. Αν έχετε ενεργοποιήσει απομακρυσμένη πρόσβαση για τους εκτυπωτές σας, τα όρια αυτά δεν ισχύουν για τους απομακρυσμένους χρήστες. Θα χρειαστεί να προσδιορίσετε με την ικανότητα `mx` και τα απομακρυσμένα αρχεία /etc/printcap. Δείτε την ενότητα Εκτυπωτές Εγκατεστημένοι σε Απομακρυσμένους Υπολογιστές για περισσότερες πληροφορίες σχετικά με τις εκτυπώσεις από απομακρυσμένους υπολογιστές.

Υπάρχει και άλλος εξειδικευμένος τρόπος περιορισμού του μεγέθους εργασιών για απομακρυσμένους εκτυπωτές. Δείτε την ενότητα Περιορισμός Εργασιών από Απομακρυσμένους Υπολογιστές.

16.4.4.4. Περιορισμός Εργασιών από Απομακρυσμένους Υπολογιστές

Το σύστημα παροχέτευσης LPD παρέχει διάφορους τρόπους περιορισμού των εργασιών από απομακρυσμένους υπολογιστές:

Παρεμπόδιση υπολογιστών

Μπορείτε να ελέγχετε από ποιους απομακρυσμένους υπολογιστές θα δέχεται αιτήσεις εκτύπωσης το τοπικό LPD, χρησιμοποιώντας τα αρχεία /etc/hosts.equiv και /etc/hosts.lpd. Το LPD ελέγχει να δει αν η εισερχόμενη αίτηση προέρχεται από έναν υπολογιστή που αναφέρεται σε κάποιο από τα δύο αρχεία. Αν όχι, το LPD απορρίπτει την αίτηση.

Η μορφή αυτών των αρχείων είναι απλή: ένα όνομα υπολογιστή ανά γραμμή. Παρατηρήστε πως το αρχείο /etc/hosts.equiv χρησιμοποιείται και από το πρωτόκολλο ruserok(3), και επηρεάζει προγράμματα όπως το rsh(1) και το rcp(1), επομένως να είστε προσεκτικοί.

Για παράδειγμα, εδώ είναι το αρχείο /etc/hosts.lpd στον υπολογιστή `rose`:

```
orchid
violet
```

```
madrigal.fishbaum.de
```

Αυτό σημαίνει πως ο `rose` δέχεται αιτήσεις από τους υπολογιστές `orchid`, `violet`, και `madrigal.fishbaum.de`. Αν κάποιος άλλος υπολογιστής προσπαθήσει να αποκτήσει πρόσβαση στο LPD του `rose`, η εργασία θα απορριφθεί.

Περιορισμοί στο Μέγεθος

Μπορείτε να ελέγχετε πόσος ελεύθερος χώρος πρέπει να απομένει στο σύστημα αρχείων όπου βρίσκεται ο κατάλογος spool. Δημιουργήστε ένα αρχείο με όνομα minfree στον κατάλογο spool για τον τοπικό εκτυπωτή. Εισάγετε σε αυτό το αρχείο έναν αριθμό που αντιπροσωπεύει πόσα blocks δίσκου (512 bytes) ελεύθερου χώρου πρέπει να υπάρχουν για να είναι δεκτή μια απομακρυσμένη εργασία.

Αυτό σας επιτρέπει να είστε βέβαιοι πως οι απομακρυσμένοι χρήστες δεν θα γεμίσουν το σύστημα αρχείων σας. Μπορείτε επίσης να το χρησιμοποιήσετε για να δώσετε μερική προτεραιότητα στους τοπικούς χρήστες: οι τοπικοί χρήστες θα μπορούν να στέλνουν εργασίες στην ουρά αναμονής ακόμη και όταν ο ελεύθερος χώρος του δίσκου έχει πέσει κάτω από τον αριθμό που αναφέρεται στο αρχείο minfree.

Για παράδειγμα, ας προσθέσουμε ένα αρχείο minfree για τον εκτυπωτή `bamboo`. Εξετάζουμε το /etc/printcap για να βρούμε τον κατάλογο spool για αυτόν τον εκτυπωτή. Εδώ είναι η καταχώριση για τον `bamboo`:

```
bamboo|ps|PS|S|panasonic|Panasonic KX-P4455 PostScript v51.4:\
        :sh:sd=/var/spool/lpd/bamboo:sc:rg=artists:mx#5000:\
        :lp=/dev/ttyu5:ms#-parenb cs8 clocal crtscts:rw:mx#5000:\
        :if=/usr/local/libexec/psif:\
        :df=/usr/local/libexec/psdf:
```

Ο κατάλογος spool καθορίζεται στην ικανότητα `sd`. Θα θέσουμε τρία megabytes (ισοδυναμεί με 6144 disk blocks) ως το μέγεθος του ελεύθερου χώρου που πρέπει να υπάρχει στο σύστημα αρχείων, ώστε το LPD να δέχεται απομακρυσμένες εργασίες:

```
# echo 6144 > /var/spool/lpd/bamboo/minfree
```

Περιορισμοί χρηστών

Μπορείτε να ελέγχετε ποιός απομακρυσμένος χρήστης μπορεί να εκτυπώνει στους τοπικούς εκτυπωτές ορίζοντας την ικανότητα `rs` στο /etc/printcap. Όταν εμφανίζεται η `rs` σε μια καταχώριση κάποιου τοπικά συνδεδεμένου εκτυπωτή, το LPD θα δεχθεί εργασίες από απομακρυσμένους υπολογιστές *αν* ο χρήστης που αποστέλλει την εργασία έχει λογαριασμό στον τοπικό υπολογιστή και με το ίδιο όνομα χρήστη. Διαφορετικά, το LPD θα απορρίψει την εργασία.

Αυτή η ικανότητα είναι ιδιαίτερα χρήσιμη σε περιβάλλοντα όπου υπάρχουν (για παράδειγμα) διαφορετικά επιχειρησιακά τμήματα που μοιράζονται το δίκτυο, και κάποιοι χρήστες πρέπει να υπερβαίνουν τα σύνορα του τμήματος. Δημιουργώντας λογαριασμούς στα συστήματα σας, θα μπορούν να χρησιμοποιούν τους εκτυπωτές σας από το δικό τους τμήμα της επιχείρησης. Αν

επιθυμείτε να τους επιτρέπετε να χρησιμοποιούν *μόνο* τους εκτυπωτές και όχι τα μηχανήματα σας, τότε μπορείτε να δημιουργήσετε λογαριασμούς "token", δίχως προσωπικούς καταλόγους και με κέλυφος που δεν μπορεί να χρησιμοποιηθεί, όπως το /usr/bin/false.

16.4.5. Καταμέτρηση Χρήσης Εκτυπωτών

Αποφασίσατε ότι χρειάζεται να χρεώνετε για τις εκτυπώσεις σας. Και γιατί όχι; Το χαρτί και το μελάνι κοστίζουν χρήματα. Και επιπλέον υπάρχει κόστος συντήρησης - οι εκτυπωτές αποτελούνται από κινητά μέρη και έχουν την τάση να χαλάνε. Έχετε εξετάσει τους εκτυπωτές σας, τον τρόπο που χρησιμοποιούνται, και το κόστος συντήρησης και έχετε υπολογίσει μια χρέωση ανά σελίδα (ή ανά μέτρο, ανά πόδι, ή άλλη μονάδα μέτρησης). Το θέμα είναι τώρα πως μπορείτε πραγματικά να ξεκινήσετε να καταμετράτε τις εκτυπώσεις σας.

Τα άσχημα νέα είναι πως το σύστημα παροχέτευσης του LPD δεν παρέχει πολύ βοήθεια σε αυτόν τον τομέα. Η καταμέτρηση εξαρτάται σε μεγάλο βαθμό από τον τύπο του εκτυπωτή που χρησιμοποιείτε, τους τύπους αρχείων που εκτυπώνετε, και τις *δικές σας* απαιτήσεις για την χρέωση των εκτυπώσεων.

Για την καταμέτρηση, θα πρέπει να μετατρέψετε το φίλτρο κειμένου (για τη χρέωση εργασιών απλού κειμένου) του εκτυπωτή και τα φίλτρα μετατροπής (για τη χρέωση όλων των άλλων τύπων αρχείων) ώστε να μετρούν σελίδες ή να ζητούν να μάθουν από τον εκτυπωτή τον αριθμό των εκτυπωμένων σελίδων. Δεν θα σας βοηθήσει ιδιαίτερα η χρήση φίλτρου εξόδου, από τη στιγμή που δεν μπορεί να κάνει καταμέτρηση. Δείτε την ενότητα Φίλτρα.

Γενικά, υπάρχουν δύο τρόποι για να κάνετε καταμέτρηση:

- Η *Περιοδική καταμέτρηση* είναι ο πιο συνηθισμένος τρόπος, πιθανώς γιατί είναι ο ευκολότερος. Κάθε φορά που κάποιος εκτυπώνει μια εργασία, το φίλτρο δημιουργεί ένα αρχείο καταγραφής όπου αναφέρει τον χρήστη, τον υπολογιστή, και τον αριθμό των σελίδων. Κάθε μήνα, εξάμηνο, χρόνο, ή άλλη χρονική περίοδο της αρεσκείας σας, συλλέγετε τα αρχεία καταγραφής για τους διάφορους εκτυπωτές, λογαριάζετε τις σελίδες που αναλογούν στους χρήστες, και χρεώνετε αναλόγως. Έπειτα σβήνετε τα στοιχεία από τα αρχεία καταγραφής, ξεκινώντας από καθαρή κατάσταση για την επόμενη περίοδο.
- Η *Καταμέτρηση κατά τη χρήση* είναι λιγότερο γνωστή, ίσως επειδή είναι πιο δύσκολος τρόπος. Σε αυτή τη μέθοδο τα φίλτρα χρεώνουν τους χρήστες για τις εκτυπώσεις τους αμέσως μόλις αυτές πραγματοποιηθούν. Όπως και με την καταγραφή χρήσης δίσκου (disk quotas), η καταμέτρηση είναι άμεση. Μπορείτε να προλαμβάνετε την χρήση εκτυπωτών από χρήστες που έχουν χτυπήσει κόκκινο, και μπορείτε να παρέχετε στους χρήστες ένα τρόπο για να ελέγχουν και να ρυθμίζουν τον "όγκο εκτυπώσεων (print quotas)." Αλλά αυτή η μέθοδος προϋποθέτει λίγο κώδικα βάσεων δεδομένων για την καταγραφή χρηστών και των εν λόγω μεγεθών.

Το σύστημα παροχέτευσης LPD υποστηρίζει εύκολα και τις δύο μεθόδους: από τη στιγμή που πρέπει εσείς να παρέχετε τα φίλτρα (τις περισσότερες φορές), θα πρέπει επίσης να παρέχετε και τον κώδικα καταμέτρησης. Αλλά υπάρχει και ένα καλό σε αυτή την υπόθεση: έχετε απεριόριστη ευελιξία στις μεθόδους καταμέτρησης. Για παράδειγμα, μπορείτε να επιλέξετε περιοδική ή κατά τη χρήση καταμέτρηση. Μπορείτε να επιλέξετε τις πληροφορίες που θα καταγράφονται: ονόματα χρηστών, ονόματα υπολογιστών, τύπους εργασιών, τυπωμένες σελίδες, τετραγωνικά μέτρα χαρτιού που χρησιμοποιήθηκε, πόσος χρόνος χρειάστηκε για να γίνει η εκτύπωση, και πολλά ακόμα. Και όλα αυτά γίνονται μετατρέποντας τα φίλτρα για να αποθηκεύουν αυτές τις πληροφορίες.

16.4.5.1. Γρήγορη και Πρόχειρη Καταμέτρηση Εκτυπώσεων

Το FreeBSD διατίθεται με δύο προγράμματα που μπορούν να παρέχουν άμεσα απλή περιοδική καταμέτρηση. Είναι το φίλτρο κειμένου `lpf`, που περιγράφεται στην ενότητα lpf: ένα Φίλτρο Κειμένου, και το pac(8), ένα πρόγραμμα που συλλέγει και αθροίζει καταχωρίσεις από αρχεία καταμετρήσεων.

Όπως αναφέραμε στην ενότητα των φίλτρων (Φίλτρα), το LPD ξεκινά τα φίλτρα κειμένου και μετατροπής περνώντας στην γραμμή εντολών του φίλτρου και το όνομα του αρχείου καταγραφής. Τα φίλτρα μπορούν να χρησιμοποιήσουν αυτή την παράμετρο για να ξέρουν που να γράφουν τις καταχωρίσεις καταμέτρησης. Το όνομα του αρχείου καταμέτρησης φαίνεται στην ικανότητα `af` στο /etc/printcap, και αν δεν ορίζεται η πλήρης διαδρομή του, χρησιμοποιείται η σχετική διαδρομή ως προς τον κατάλογο spool.

Το LPD ξεκινά το `lpf` με παραμέτρους πλάτους και μήκους σελίδας (από τις ικανότητες `pw` και `pl`). Το `lpf` χρησιμοποιεί αυτές τις παραμέτρους για να προσδιορίσει την ποσότητα χαρτιού που χρησιμοποιήθηκε. Μετά την αποστολή του αρχείου στον εκτυπωτή, γράφει μια καταχώριση καταμέτρησης στο αρχείο καταγραφής. Οι καταχωρίσεις μοιάζουν με τις παρακάτω:

```
2.00 rose:andy
3.00 rose:kelly
3.00 orchid:mary
5.00 orchid:mary
2.00 orchid:zhang
```

Θα πρέπει να χρησιμοποιείτε ξεχωριστό αρχείο καταγραφής για κάθε εκτυπωτή, αφού το `lpf` δεν έχει ενσωματωμένη δυνατότητα κλειδώματος αρχείου (file locking), και δύο `lpf` μπορούν να καταστρέψουν το ένα την καταχώριση του άλλου αν πρόκειται να γράψουν ταυτόχρονα στο ίδιο αρχείο. Ένας εύκολος τρόπος για να βεβαιώσετε την μοναδικότητα αρχείου καταγραφής ανά εκτυπωτή είναι να χρησιμοποιήσετε την ικανότητα `af=acct` στο /etc/printcap. Έτσι, κάθε αρχείο καταγραφής θα βρίσκεται στον κατάλογο spool του αντίστοιχου εκτυπωτή, σε ένα αρχείο με όνομα acct.

Όταν είστε έτοιμοι να χρεώσετε τους χρήστες για τις εκτυπώσεις, εκτελέστε το πρόγραμμα pac(8). Απλά μεταβείτε στον κατάλογο spool για τον εκτυπωτή που κάνετε καταμέτρηση και πληκτρολογήστε `pac`. Θα εμφανιστεί ένας απολογισμός με χρεώσεις σε δολάρια, όπως βλέπετε στη συνέχεια:

```
  Login               pages/feet   runs    price
orchid:kelly               5.00     1   $  0.10
orchid:mary               31.00     3   $  0.62
orchid:zhang               9.00     1   $  0.18
rose:andy                  2.00     1   $  0.04
rose:kelly               177.00   104   $  3.54
rose:mary                 87.00    32   $  1.74
rose:root                 26.00    12   $  0.52

total                    337.00   154   $  6.74
```

Παρακάτω είναι οι παράμετροι που δέχεται το pac(8):

-Pprinter

Για ποιό *printer* να κάνει απολογισμό. Αυτή η επιλογή δουλεύει μόνο αν υπάρχει η πλήρης διαδρομή στην ικανότητα `af` στο /etc/printcap.

-c

Ταξινομεί το αποτέλεσμα ανά κόστος αντί της αλφαβητικής ταξινόμησης των χρηστών.

-m

Αγνοεί το όνομα του υπολογιστή στα αρχεία καταγραφής. Με αυτή την επιλογή, ο χρήστης `smith` στον υπολογιστή `alpha` είναι ο ίδιος χρήστης με τον `smith` στον υπολογιστή `gamma`. Χωρίς την επιλογή αυτή, είναι διαφορετικοί χρήστες.

-pprice

Υπολογίζει τις χρεώσεις με *price* (τιμή) σε δολάρια ανά σελίδα ή ανά πόδι αντί για την τιμή από την ικανότητα `pc` στο /etc/printcap, ή αλλιώς δύο σεντς (από προεπιλογή). Μπορείτε να ορίσετε ως *price* μια τιμή με δεκαδικά ψηφία (floating point).

-r

Αντιστρέφει την σειρά ταξινόμησης.

-s

Δημιουργεί ένα αρχείο απολογισμού των καταμετρήσεων και καθαρίζει τα περιεχόμενα των αρχείων καταγραφής.

name...

Τυπώνει πληροφορίες αναφοράς μόνο για τα συγκεκριμένα *name* (ονόματα) χρηστών.

Στον προεπιλεγμένο απολογισμό που παράγει το pac(8), βλέπετε των αριθμό των τυπωμένων σελίδων ανά χρήστη από τους διάφορους υπολογιστές. Αν, στο χώρο σας, ο υπολογιστής δεν έχει σημασία (γιατί οι χρήστες μπορούν να χρησιμοποιήσουν οποιονδήποτε θέλουν), εκτελέστε την εντολή `pac -m`, για να δημιουργήσετε τον ακόλουθο απολογισμό:

```
  Login               pages/feet   runs    price
andy                        2.00     1   $  0.04
kelly                     182.00   105   $  3.64
mary                      118.00    35   $  2.36
root                       26.00    12   $  0.52
zhang                       9.00     1   $  0.18

total                     337.00   154   $  6.74
```

Για τον ορισμό ποσοστού χρέωσης σε δολάρια, το pac(8) χρησιμοποιεί την ικανότητα `pc` στο αρχείο /etc/printcap (προεπιλεγμένη τιμή 200, ή 2 σεντς ανά σελίδα). Προσδιορίστε σε αυτήν την ικανότητα, σε εκατοστά του σεντ, την τιμή ανά σελίδα ή ανά πόδι που θέλετε να χρεώνετε για τις εκτυπώσεις. Μπορείτε να προσπεράσετε αυτή την τιμή όταν τρέχετε το pac(8) με την επιλογή `-p`. Η μονάδα μέτρησης για την επιλογή `-p` είναι σε δολάρια, όχι σε εκατοστά του σεντ. Για παράδειγμα,

```
# pac -p1.50
```

```
ορίζει κόστος κάθε σελίδας ένα δολάριο και πενήντα σεντς. Μπορείτε πραγματικά να έχετε
πολλά έσοδα χρησιμοποιώντας αυτές τις χρεώσεις.
```

Τέλος, εκτελώντας `pac -s` θα αποθηκεύσετε τις πληροφορίες του απολογισμού σε ένα αρχείο καταγραφής απολογισμού, που θα έχει το ίδιο όνομα με το αρχείο καταγραφής του εκτυπωτή, αλλά με κατάληξη `_sum`. Έπειτα καθαρίζεται το αρχείο καταγραφής. Όταν εκτελέσετε πάλι το pac(8), θα ξαναδιαβάσει το αρχείο απολογισμού, για να πάρει τα αρχικά σύνολα, και θα προσθέσει τις πληροφορίες από το κανονικό αρχείο καταγραφής.

16.4.5.2. Πως Μπορείτε να Μετρήσετε τις Τυπωμένες Σελίδες;

Για να μετρήσετε τις τυπωμένες σελίδες με έστω στοιχειώδη λεπτομέρεια, θα πρέπει να προσδιορίσετε πόσο χαρτί χρειάζεται μια εργασία. Αυτό είναι το ουσιαστικότερο πρόβλημα στην καταμέτρηση εκτυπώσεων.

Για εργασίες απλού κειμένου, το πρόβλημα δεν είναι δύσκολο να λυθεί: Μετράτε πόσες γραμμές υπάρχουν σε μια εργασία και τις συγκρίνετε με πόσες γραμμές μπορεί να τυπώσει ο εκτυπωτής σας σε μια σελίδα. Μην ξεχάσετε να συμπεριλάβετε τα backspaces που προκαλούν υπερτύπωση, ή επιμήκης λογικές γραμμές που αναδιπλώνονται σε περισσότερες από μία φυσικές γραμμές.

Το φίλτρο κειμένου `lpf` (που παρουσιάσαμε στο lpf: ένα Φίλτρο Κειμένου) λαμβάνει υπόψιν του αυτά τα στοιχεία όταν κάνει καταμέτρηση. Αν γράφετε κάποιο φίλτρο κειμένου που χρειάζεται να κάνει καταμέτρηση, ίσως να θέλετε να ελέγξετε τον πηγαίο κώδικα του `lpf`.

Πως χειρίζεστε όμως τους υπόλοιπους τύπους αρχείων;

Για τις μετατροπές από DVI-σε-LaserJet ή από DVI-σε-PostScript®, μπορείτε να κάνετε το φίλτρο σας να αναλύει την έξοδο του `dvilj` ή του `dvips` και να ελέγχει πόσες σελίδες δημιουργήθηκαν από τη μετατροπή. Ίσως μπορέσετε να κάνετε κάτι παρόμοιο και με διαφορετικούς τύπους αρχείων και προγράμματα μετατροπής

Ωστόσο, όλες αυτές οι μέθοδοι έχουν το μειονέκτημα πως ο εκτυπωτής πιθανώς στην πραγματικότητα να μην εκτυπώσει όλες τις σελίδες. Για παράδειγμα, θα μπορούσε να μπλοκαριστεί το χαρτί, ή να τελειώσει το τόνερ, ή ακόμη να συμβεί και έκρηξη -ενώ ο χρήστης θα συνεχίσει να χρεώνεται.

Τι θα μπορούσατε να κάνετε;

Υπάρχει μόνο ένας *σίγουρος* τρόπος για να κάνετε καταμέτρηση *ακριβείας*. Να πάρετε έναν εκτυπωτή που να μπορεί να σας πει πόσο χαρτί χρησιμοποιεί, και να τον συνδέσετε μέσω σειριακής θύρας ή μέσω δικτύου. Σχεδόν όλοι οι εκτυπωτές PostScript® υποστηρίζουν αυτή την δυνατότητα. Θα βρείτε και άλλους τύπους και κατασκευαστές που κάνουν επίσης το ίδιο (για παράδειγμα, οι laser εκτυπωτές δικτύου της Imagen). Μετατρέψτε τα φίλτρα για αυτούς τους εκτυπωτές ώστε να καταγράφουν τις τυπωμένες σελίδες μετά την ολοκλήρωση της εκάστοτε εργασίας εκτύπωσης, και ρυθμίστε τους να κρατούν αρχεία καταγραφής με *μόνο* αυτή την πληροφορία. Δεν χρειάζεται

καταμέτρηση γραμμών ούτε αναφορά σφαλμάτων.

Φυσικά, πάντα έχετε τη δυνατότητα να φανείτε γενναιόδωρος και να παρέχετε τις εκτυπώσεις σας δωρεάν.

16.5. Χρήση Εκτυπωτών

Αυτή η ενότητα περιγράφει πως να χρησιμοποιείτε τους εκτυπωτές που έχετε εγκαταστήσει στο FreeBSD. Οι βασικές εντολές για τον τελικό χρήστη είναι οι ακόλουθες:

lpr(1)

Εκτύπωση εργασιών

lpq(1)

Έλεγχος ουράς αναμονής (print queue) του εκτυπωτή

lprm(1)

Διαγραφή εργασιών από την ουρά αναμονής

Υπάρχει επίσης μια εντολή για τους διαχειριστές, η lpc(8), που περιγράφεται στην ενότητα Διαχείριση Εκτυπωτών, και χρησιμοποιείται για να ελέγχει τους εκτυπωτές και τις ουρές αναμονής.

Και οι τρεις εντολές lpr(1), lprm(1), και lpq(1) δέχονται την επιλογή `-P printer-name` με την οποία καθορίζεται σε ποιον εκτυπωτή ή ουρά αναμονής θα ενεργήσουν, όπως αναφέρεται στο αρχείο /etc/printcap. Αυτό σας επιτρέπει να αποστείλετε, να διαγράψετε, και να ελέγξετε εργασίες σε διάφορους εκτυπωτές. Αν δεν χρησιμοποιείτε την επιλογή `-P`, τότε οι εντολές χρησιμοποιούν τον εκτυπωτή που αναφέρεται στη μεταβλητή περιβάλλοντος `PRINTER`. Τέλος, αν δεν έχετε θέσει μια μεταβλητή περιβάλλοντος `PRINTER`, οι εντολές εκτελούνται με τον προεπιλεγμένο εκτυπωτή που ονομάζεται `lp`.

Από δω και στο εξής, με την ορολογία *προεπιλεγμένος εκτυπωτής* θα εννοούμε τον εκτυπωτή που αναφέρεται στην μεταβλητή περιβάλλοντος `PRINTER`, ή αν δεν υπάρχει, τον εκτυπωτή με το όνομα `lp`.

16.5.1. Εκτύπωση Εργασιών

Για να εκτυπώσετε αρχεία, πληκτρολογήστε:

```
% lpr filename ...
```

Θα εκτυπωθούν όλα τα αναφερόμενα αρχεία στον προεπιλεγμένο εκτυπωτή. Αν δεν αναφέρετε αρχεία, το lpr(1) διαβάζει δεδομένα από το standard input. Για παράδειγμα, αυτή η εντολή θα εκτυπώσει μερικά σημαντικά αρχεία του συστήματος:

```
% lpr /etc/host.conf /etc/hosts.equiv
```

Για να επιλέξετε ένα συγκεκριμένο εκτυπωτή, πληκτρολογήστε:

```
% lpr -P printer-name filename ...
```

Στο παράδειγμα μας θα εκτυπωθεί μια μεγάλη λίστα αρχείων του τρέχοντος καταλόγου στον εκτυπωτή που ονομάζεται `rattan`:

```
% ls -l | lpr -P rattan
```

Αφού δεν αναφέρονται ονόματα αρχείων στην εντολή lpr(1), το `lpr` διαβάζει τα δεδομένα που θα εκτυπώσει από το standard input, τα οποία είναι η έξοδος της εντολής `ls -l`.

Η εντολή lpr(1) μπορεί να δεχθεί ένα μεγάλο αριθμό επιλογών για να ελέγχει την μορφοποίηση, να μετατρέπει αρχεία, να δημιουργεί πολλαπλά αντίγραφα, κ.λ.π. Για περισσότερες πληροφορίες, δείτε την ενότητα Επιλογές Εκτύπωσης.

16.5.2. Έλεγχος Εργασιών

Όταν εκτυπώνετε με το lpr(1), τα δεδομένα που θέλετε να εκτυπώσετε τοποθετούνται σε ένα πακέτο (package) που ονομάζεται "εργασία εκτύπωσης (print job)", η οποία αποστέλλεται στο σύστημα παροχέτευσης LPD. Κάθε εκτυπωτής έχει μια ουρά αναμονής εργασιών, και η εργασία σας αναμένει μαζί με άλλες δικές σας και άλλων χρηστών. Ο εκτυπωτής τις εκτυπώνει με την σειρά άφιξης στην ουρά αναμονής.

Για να εμφανίσετε την ουρά αναμονής για τον προεπιλεγμένο εκτυπωτή, πληκτρολογήστε lpq(1). Για κάποιον συγκεκριμένο εκτυπωτή, χρησιμοποιήστε την επιλογή `-P`. Για παράδειγμα, η εντολή:

```
% lpq -P bamboo
```

εμφανίζει την ουρά αναμονής για τον εκτυπωτή με το όνομα `bamboo`. Ακολουθεί ένα παράδειγμα εξόδου της εντολής `lpq`:

```
bamboo is ready and printing
Rank   Owner    Job  Files                              Total Size
active kelly    9    /etc/host.conf, /etc/hosts.equiv   88 bytes
2nd    kelly    10   (standard input)                   1635 bytes
3rd    mary     11   ...                                78519 bytes
```

Εμφανίζονται τρεις εργασίες στη λίστα αναμονής για τον `bamboo`. Στην πρώτη εργασία, που έχει σταλεί από τον χρήστη kelly, έχει αποδοθεί ο "αριθμός εργασίας (job number)" 9. Κάθε εργασία ενός εκτυπωτή χαρακτηρίζεται από ένα μοναδικό τέτοιο αριθμό. Τις περισσότερες φορές μπορείτε να τον αγνοήσετε, αλλά θα τον χρειαστείτε αν θέλετε να διαγράψετε κάποια εργασία. Δείτε την ενότητα Διαγραφή Εργασιών για περισσότερες πληροφορίες.

Η εργασία με το νούμερο εννέα αποτελείται από δύο αρχεία. Τα πολλαπλά αρχεία που δόθηκαν στη γραμμή εντολών του lpr(1) θεωρούνται μέρος μίας μόνο εργασίας. Αυτή είναι και η τρέχουσα ενεργή εργασία (παρατηρήστε τη λέξη `active` της στήλης "Rank"), που σημαίνει πως η εργασία

εκτυπώνεται αυτή τη στιγμή. Η δεύτερη εργασία αποτελείται από δεδομένα που έχουν περάσει στην standard input της εντολής lpr(1). Η τρίτη εργασία προέρχεται από τον χρήστη `mary`, και πρόκειται για μια πολύ ογκώδη εργασία. Το όνομα διαδρομής του αρχείου που πρόκειται να εκτυπωθεί είναι πολύ μεγάλο για να χωρέσει στη στήλη, και για αυτό η εντολή lpq(1) απλά το συμβολίζει με τρεις τελείες.

Η πρώτη γραμμή της εξόδου από την lpq(1) είναι επίσης πολύ χρήσιμη: μας ενημερώνει για το τι κάνει την παρούσα στιγμή ο εκτυπωτής (ή τουλάχιστον για το τι πιστεύει το LPD πως κάνει ο εκτυπωτής αυτή τη στιγμή).

Η εντολή lpq(1) επίσης υποστηρίζει την επιλογή `-l` για να δημιουργήσει μια μεγάλη, λεπτομερή λίστα. Ακολουθεί ένα παράδειγμα του `lpq -l`:

```
waiting for bamboo to become ready (offline ?)
kelly: 1st              [job 009rose]
       /etc/host.conf                   73 bytes
       /etc/hosts.equiv                 15 bytes

kelly: 2nd              [job 010rose]
       (standard input)                 1635 bytes

mary: 3rd                               [job 011rose]
      /home/orchid/mary/research/venus/alpha-regio/mapping 78519 bytes
```

16.5.3. Αφαίρεση Εργασιών

Αν αλλάξετε γνώμη για μια εργασία που είχατε αποστείλει προς εκτύπωση, μπορείτε να την αφαιρέσετε από την λίστα αναμονής με την εντολή lprm(1). Μπορείτε ακόμη να χρησιμοποιήσετε την lprm(1) για να αφαιρέσετε μια ενεργή εργασία, αλλά πιθανόν κάποιο μέρος της να εκτυπωθεί έτσι και αλλιώς.

Για να αφαιρέσετε μια εργασία από τον προεπιλεγμένο εκτυπωτή, χρησιμοποιήστε πρώτα την lpq(1) για να βρείτε τον αριθμό της. Έπειτα πληκτρολογήστε:

```
% lprm job-number
```

Για να αφαιρέσετε μια εργασία από κάποιον συγκεκριμένο εκτυπωτή, προσθέστε την επιλογή `-P`. Η ακόλουθη εντολή αφαιρεί την εργασία με αριθμό 10 από την ουρά αναμονής για τον εκτυπωτή `bamboo`:

```
% lprm -P bamboo 10
```

Η εντολή lprm(1) έχει μερικές συντομεύσεις:

lprm -

Αφαιρεί όλες τις εργασίες (για τον προεπιλεγμένο εκτυπωτή) που ανήκουν σε εσάς.

lprm *user*

Αφαιρεί όλες τις εργασίες (για τον προεπιλεγμένο εκτυπωτή) που ανήκουν στον *χρήστη (user)*. Ο υπερχρήστης (superuser) μπορεί να αφαιρέσει εργασίες άλλων χρηστών, εσείς μπορείτε να αφαιρέσετε μόνο τις δικές σας.

lprm

Η εντολή lprm(1) χωρίς αριθμό εργασίας, όνομα χρήστη, ή `-` που εμφανίζεται στην γραμμή εντολών, αφαιρεί την τρέχουσα ενεργή εργασία στον προεπιλεγμένο εκτυπωτή, αν ανήκει σε σάς. Ο υπερχρήστης (superuser) μπορεί να αφαιρέσει οποιαδήποτε ενεργή εργασία.

Για να δουλέψετε σε κάποιον συγκεκριμένο εκτυπωτή αντί του προεπιλεγμένου, απλά χρησιμοποιήστε την επιλογή `-P` με τις παραπάνω συντομεύσεις. Για παράδειγμα, η ακόλουθη εντολή αφαιρεί όλες τις εργασίες του τρέχοντος χρήστη από την ουρά αναμονής του εκτυπωτή `rattan`:

```
% lprm -P rattan -
```

Αν εργάζεστε σε περιβάλλον δικτύου, η lprm(1) θα σας επιτρέψει να αφαιρέσετε εργασίες μόνο από τον υπολογιστή που τις έχετε στείλει, ανεξάρτητα αν ο εκτυπωτής είναι προσβάσιμος και από άλλους υπολογιστές. Η ακόλουθη εντολή επιδεικνύει ακριβώς αυτό το χαρακτηριστικό:

```
% lpr -P rattan myfile
% rlogin orchid
% lpq -P rattan
Rank   Owner      Job  Files                         Total Size
active seeyan     12    ...                           49123 bytes
2nd    kelly      13   myfile                         12 bytes
% lprm -P rattan 13
rose: Permission denied
% logout
% lprm -P rattan 13
dfA013rose dequeued
cfA013rose dequeued
```

16.5.4. Πέρα από το Απλό Κείμενο: Περισσότερες Επιλογές Εκτύπωσης

Η εντολή lpr(1) υποστηρίζει μια γκάμα επιλογών για τον έλεγχο μορφοποίησης κειμένου, μετατροπής γραφικών και άλλων μορφών αρχείων, παραγωγής πολλαπλών αντιγράφων, χειρισμού εργασιών, και άλλα. Οι επιλογές αυτές περιγράφονται στην παρούσα ενότητα.

16.5.4.1. Επιλογές Μορφοποίησης και Μετατροπής

Οι ακόλουθες επιλογές της lpr(1) ελέγχουν την μορφοποίηση των αρχείων της εργασίας εκτύπωσης. Χρησιμοποιήστε τις αν η εργασία σας δεν περιέχει απλό κείμενο ή αν επιθυμείτε να μορφοποιήσετε απλό κείμενο διαμέσου του εργαλείου pr(1).

Για παράδειγμα, η ακόλουθη εντολή τυπώνει ένα αρχείο DVI (από το σύστημα στοιχειοθεσίας TeX)

με όνομα fish-report.dvi στον εκτυπωτή με όνομα bamboo:

```
% lpr -P bamboo -d fish-report.dvi
```

Αυτές οι επιλογές εφαρμόζονται σε κάθε αρχείο της εργασίας, και έτσι δεν μπορείτε να αναμίξετε (ας πούμε) αρχεία DVI και ditroff μαζί στην ίδια εργασία. Απλώς στείλτε τα αρχεία σαν διαφορετικές εργασίες, χρησιμοποιώντας διαφορετικές επιλογές μετατροπής για κάθε εργασία.

Όλες αυτές οι επιλογές εκτός της -p και της -T απαιτούν εγκατεστημένα φίλτρα μετατροπής για τον εκτυπωτή προορισμού. Για παράδειγμα, η επιλογή -d απαιτεί το φίλτρο μετατροπής DVI. Η ενότητα Φίλτρα Μετατροπής δίνει περισσότερες λεπτομέρειες.

-c

Εκτυπώνει αρχεία cifplot.

-d

Εκτυπώνει αρχεία DVI.

-f

Εκτυπώνει αρχεία κειμένου FORTRAN.

-g

Εκτυπώνει δεδομένα σχεδίασης (plot).

-i number

Εκτυπώνει την έξοδο με εσοχή *number* στηλών. Αν παραλείψετε το *number*, η εσοχή θα είναι 8 στήλες. Αυτή η επιλογή δουλεύει μόνο με ορισμένα φίλτρα μετατροπής.

Μην τοποθετείτε κενό διάστημα μεταξύ του -i και του αριθμού.

-l

Εκτυπώνει δεδομένα κειμένου κατά γράμμα (literal), συμπεριλαμβάνοντας και τους χαρακτήρες ελέγχου.

-n

Εκτυπώνει δεδομένα ditroff (δεδομένα troff ανεξάρτητα από τη συσκευή).

-p

Μορφοποιεί το απλό κείμενο με την pr(1) πριν να το εκτυπώσει. Δείτε την pr(1) για περισσότερες πληροφορίες.

-T title

Χρησιμοποιεί το *title* στην κεφαλίδα του pr(1) αντί για το όνομα αρχείου. Αυτή η επιλογή επιδρά μόνο όταν χρησιμοποιείται με την επιλογή -p

`-t`

Εκτυπώνει δεδομένα troff.

`-v`

Εκτυπώνει δεδομένα ράστερ.

Εδώ είναι ένα παράδειγμα: αυτή η εντολή εκτυπώνει μια κομψά μορφοποιημένη έκδοση της σελίδας βοηθείας ls(1) στον προεπιλεγμένο εκτυπωτή:

```
% zcat /usr/shared/man/man1/ls.1.gz | troff -t -man | lpr -t
```

Η εντολή zcat(1) αποσυμπιέζει τον πηγαίο κώδικα της σελίδας βοηθείας ls(1) και τον περνάει στην εντολή troff(1), η οποία τον μορφοποιεί και δημιουργεί στην έξοδο της δεδομένα GNU troff, τα αποστέλλει στην lpr(1), η οποία με τη σειρά της αποστέλλει την εργασία στο LPD. Επειδή χρησιμοποιήσαμε την επιλογή `-t` στο lpr(1), ο spooler, κατά τη διάρκεια της εκτύπωσης, θα μετατρέψει την έξοδο GNU troff σε ένα τύπο δεδομένων κατανοητό από τον προεπιλεγμένο εκτυπωτή.

16.5.4.2. Επιλογές Χειρισμού Εργασιών

Οι ακόλουθες επιλογές του lpr(1) οδηγούν το LPD να χειριστεί τις εργασίες με ειδικό τρόπο:

-# *copies*

Δημιουργεί έναν αριθμό *copies* (αντιγράφων) για κάθε αρχείο της εργασίας αντί για ένα μόνο αντίγραφο. Ο διαχειριστής μπορεί να απενεργοποιήσει αυτή την επιλογή για να μειώσει την καταπόνηση των εκτυπωτών και να ενθαρρύνει την χρήση φωτοτυπικών μηχανημάτων. Δείτε την ενότητα Περιορισμός Εκτύπωσης Πολλαπλών Αντιγράφων.

Σε αυτό το παράδειγμα, εκτυπώνουμε στον προεπιλεγμένο εκτυπωτή τρία αντίγραφα του parser.c και τρία αντίγραφα του parser.h:

```
% lpr -#3 parser.c parser.h
```

-m

Αποστολή mail μετά την ολοκλήρωση εκτύπωσης της εργασίας. Με αυτή την επιλογή, το σύστημα LPD στέλνει mail στο λογαριασμό σας μόλις ολοκληρωθεί ο χειρισμός εκτύπωσης της εργασίας σας. Στο μήνυμα του, θα σας ενημερώσει αν η εργασία ολοκληρώθηκε επιτυχώς ή αν παρουσιάστηκε σφάλμα και (συχνά) ποιό ήταν το σφάλμα.

-s

Δεν αντιγράφει τα αρχεία στον κατάλογο spool, αλλά αντί για αυτό, δημιουργεί συμβολικές συντομεύσεις (symbolic links) προς αυτά.

Αν εκτυπώνετε μια μεγάλη εργασία, ίσως θέλετε να χρησιμοποιήσετε αυτή την επιλογή. Θα σας γλυτώσει χώρο στον κατάλογο spool (ίσως η εργασία σας να υπερβαίνει τον ελεύθερο χώρο του συστήματος αρχείων που περιέχει τον κατάλογο spool). Επίσης θα κερδίσετε χρόνο αφού το LPD δεν θα χρειαστεί να αντιγράψει όλη την εργασία σας στον κατάλογο spool.

Αυτό, ωστόσο, έχει και ένα μειονέκτημα: από τη στιγμή που το LPD θα κάνει αναφορά κατευθείαν στο πρωτότυπο αρχείο, δεν θα έχετε δυνατότητα να μετατρέψετε ή να διαγράψετε το αρχείο έως ότου εκτυπωθεί.

Αν εκτυπώνετε σε ένα απομακρυσμένο εκτυπωτή, το LPD πιθανώς θα χρειαστεί τελικά να αντιγράψει τα αρχεία από τον τοπικό υπολογιστή στον απομακρυσμένο, επομένως η επιλογή `-s` σε αυτή την περίπτωση εξοικονομεί χώρο στον τοπικό κατάλογο spool, αλλά όχι στον απομακρυσμένο. Εξακολουθεί ωστόσο να είναι ιδιαίτερα χρήσιμη.

-r

Απομακρύνει τα αρχεία της εργασίας μετά την αντιγραφή τους στον κατάλογο spool, ή μετά την εκτύπωση τους με την επιλογή `-s`. Να είστε προσεκτικοί με αυτή την επιλογή!

16.5.4.3. Επιλογές Σελίδων Κεφαλίδας

Αυτές οι επιλογές του lpr(1) ρυθμίζουν το κείμενο που κανονικά εμφανίζεται στην σελίδα κεφαλίδας της εργασίας. Αν οι σελίδες κεφαλίδας παρεμποδίζονται για τον συγκεκριμένο εκτυπωτή, αυτές οι επιλογές δεν έχουν καμία επίδραση. Δείτε την ενότητα Σελίδες Κεφαλίδας για πληροφορίες σχετικά με τις ρυθμίσεις των σελίδων κεφαλίδας.

-C *text*

Αντικαθιστά το όνομα υπολογιστή στη σελίδα κεφαλίδας με *text*. Το όνομα υπολογιστή που εμφανίζεται είναι, από προεπιλογή, το όνομα του υπολογιστή από τον οποίο έγινε η αποστολή της εργασίας.

-J *text*

Αντικαθιστά το όνομα εργασίας στη σελίδα κεφαλίδας με *text*. Το όνομα εργασίας που εμφανίζεται από προεπιλογή, είναι το όνομα του πρώτου αρχείου της εργασίας, ή stdin αν η εκτύπωση γίνεται από το standard input.

-h

Δεν εκτυπώνει σελίδα κεφαλίδας.

Ανάλογα με τις ρυθμίσεις, αυτή η επιλογή ίσως να μην έχει επίδραση λόγω του τρόπου με τον οποίο δημιουργούνται οι σελίδες κεφαλίδας. Για περισσότερες λεπτομέρειες, δείτε την ενότητα Σελίδες Κεφαλίδας.

16.5.5. Διαχείριση Εκτυπωτών

Ως διαχειριστής, χρειάστηκε να εγκαταστήσετε, να ρυθμίσετε και να δοκιμάσετε τους εκτυπωτές σας. Χρησιμοποιώντας την εντολή lpc(8), μπορείτε να επικοινωνήσετε με τους εκτυπωτές σας με ακόμη περισσότερους τρόπους. Με την lpc(8), μπορείτε:

- Να εκκινείτε και να σταματάτε τους εκτυπωτές
- Να ενεργοποιείτε και να απενεργοποιείτε τις ουρές αναμονής
- Να ανακατατάσσετε την σειρά εργασιών σε κάθε ουρά αναμονής.

Καταρχήν, μία σημείωση σχετικά με την ορολογία: αν ένας εκτυπωτής είναι *σταματημένος (stopped)*, δεν θα εκτυπώσει τίποτε από την ουρά αναμονής εργασιών. Οι χρήστες μπορούν ακόμη να στέλνουν εργασίες, οι οποίες μπαίνουν στην ουρά αναμονής έως ότου ο εκτυπωτής *ξεκινήσει* ή καθαριστεί η ουρά αναμονής.

Αν έχει *απενεργοποιηθεί* η ουρά αναμονής, κανείς χρήστης (εκτός του `root`) δεν μπορεί να αποστείλει εργασίες στον εκτυπωτή. Μια *ενεργή* ουρά αναμονής επιτρέπει να αποσταλούν εργασίες στον εκτυπωτή. Ένας εκτυπωτής μπορεί να *ξεκινήσει* με ουρά αναμονής απενεργοποιημένη, και σε αυτή την περίπτωση θα συνεχίσει να εκτυπώνει τις εργασίες της ουράς έως ότου αυτή αδειάσει.

Γενικά, πρέπει να έχετε προνόμια `root` για να χρησιμοποιήσετε την εντολή lpc(8). Οι κανονικοί χρήστες μπορούν να χρησιμοποιούν την εντολή lpc(8) μόνο για να βλέπουν την κατάσταση του εκτυπωτή και να επανεκκινούν τον εκτυπωτή σε περίπτωση μπλοκαρίσματος.

Παρακάτω θα βρείτε μια λίστα εντολών του lpc(8). Οι περισσότερες από τις εντολές παίρνουν ως παράμετρο το *printer-name* για τη ρύθμιση του συγκεκριμένου εκτυπωτή. Μπορείτε να χρησιμοποιείτε `all` στη θέση του *printer-name* για να αναφερθείτε σε όλους τους εκτυπωτές που είναι καταχωρισμένοι στο /etc/printcap.

`abort printer-name`

Διαγράφει την τρέχουσα εργασία και σταματάει τον εκτυπωτή. Οι χρήστες μπορούν ακόμη να αποστείλουν εργασίες αν η ουρά αναμονής είναι ακόμη ενεργή.

`clean printer-name`

Διαγράφει τα παλιά αρχεία από τον κατάλογο spool του εκτυπωτή. Σε κάποιες περιπτώσεις, τα αρχεία από τα οποία αποτελείται κάποια εργασία δεν αφαιρούνται κανονικά από το LPD, ειδικά αν υπήρξαν σφάλματα κατά την εκτύπωση ή κάποιες ενέργειες από τον διαχειριστή. Αυτή η εντολή βρίσκει αρχεία που δεν ανήκουν στον κατάλογο spool και τα αφαιρεί.

`disable printer-name`

Απενεργοποιεί την ουρά αναμονής για νέες εργασίες. Αν ο εκτυπωτής δουλεύει, θα συνεχίσει να εκτυπώνει τις εναπομείναντες εργασίες στην ουρά αναμονής. Ο superuser (`root`) μπορεί πάντα να στέλνει εργασίες, ακόμη και σε απενεργοποιημένη σειρά αναμονής.

Αυτή η εντολή είναι χρήσιμη, όταν ελέγχετε ένα νέο εκτυπωτή ή όταν εγκαθιστάτε ένα φίλτρο: απενεργοποιήστε την ουρά αναμονής και στείλτε εργασίες σαν `root`. Οι υπόλοιποι χρήστες δεν θα έχουν δυνατότητα να αποστείλουν εργασίες έως ότου ολοκληρώσετε τους ελέγχους σας και επανενεργοποιήσετε την ουρά αναμονής με την εντολή `enable`.

`down printer-name message`

Οδηγεί τον εκτυπωτή σε "κατέβασμα" (down). Είναι ισοδύναμο με το `disable` ακολουθούμενο από ένα `stop`. Το *message* (μήνυμα) εμφανίζεται όταν κάποιος χρήστης ελέγχει την σειρά αναμονής με lpq(1) ή την κατάσταση του εκτυπωτή με `lpc status`.

`enable printer-name`

Ενεργοποίηση της ουράς αναμονής του εκτυπωτή. Οι χρήστες μπορούν να αποστείλουν εργασίες αλλά ο εκτυπωτής δεν θα τυπώσει έως ότου ξεκινήσει.

`help command-name`

Τυπώνει σελίδες βοηθείας για την εντολή *command-name*. Δίχως το *command-name*, εκτυπώνει μια περίληψη όλων των διαθέσιμων εντολών.

`restart printer-name`

Ξεκινά τον εκτυπωτή. Οι κανονικοί χρήστες μπορούν να χρησιμοποιήσουν αυτή την εντολή μόνο σε κάποια ειδική περίπτωση που το LPD δεν αποκρίνεται, αλλά δεν μπορούν να ξεκινήσουν ένα εκτυπωτή που έχει σταματήσει εξαιτίας των εντολών `stop` ή `down`. Η εντολή `restart` είναι ισοδύναμη με την `abort` ακολουθούμενη από τη `start`.

`start printer-name`

Ξεκινά τον εκτυπωτή. Ο εκτυπωτής θα τυπώσει εργασίες από την ουρά αναμονής του.

`stop printer-name`

Σταματάει τον εκτυπωτή. Ο εκτυπωτής θα ολοκληρώσει την τρέχουσα εργασία του και δεν θα τυπώσει καμία άλλη εργασία από την ουρά αναμονής του. Ακόμη και αν ο εκτυπωτής είναι σταματημένος, οι χρήστες μπορούν ακόμη να στέλνουν εργασίες αν είναι ενεργοποιημένη η ουρά αναμονής.

`topq printer-name job-or-username`

Ανακατάταξη της ουράς αναμονής για τον *printer-name*. Τοποθετούνται πρώτες οι εργασίες με αριθμό αναφοράς *job* ή αυτές που ανήκουν στο χρήστη *username*. Για αυτή την εντολή, δεν μπορείτε να χρησιμοποιήσετε `all` στην θέση του *printer-name*.

`up printer-name`

Οδηγεί τον εκτυπωτή σε "ανέβασμα" (up). Το αντίθετο της εντολής `down`. Ισοδυναμεί με την `start` ακολουθούμενη από την εντολή `enable`.

Το lpc(8) δέχεται τις παραπάνω εντολές στην γραμμή εντολών. Αν δεν εισάγετε καμία εντολή, το lpc(8) μπαίνει σε κατάσταση αλληλεπίδρασης (interactive), όπου μπορείτε να πληκτρολογείτε εντολές μέχρι να δώσετε `exit`, `quit`, ή end-of-file.

16.6. Εναλλακτικές Λύσεις για τον Στάνταρ Spooler

Αν έχετε μελετήσει πιστά όλο το κεφάλαιο μέχρι εδώ, θα έχετε μάθει σχεδόν τα πάντα σχετικά με το σύστημα παροχέτευσης LPD που διατίθεται με το FreeBSD. Θα έχετε κατανοήσει και πολλές από τις ελλείψεις του, που φυσικά γεννούν το ερώτημα: "Ποια άλλα συστήματα παροχέτευσης (που να λειτουργούν στο FreeBSD) υπάρχουν διαθέσιμα;"

LPRng

Το LPRng, το οποίο σκόπιμα σημαίνει "LPR: the Next Generation (η Επόμενη Γενιά)" είναι μια από την αρχή υλοποίηση του PLP. Ο Patrick Powell και ο Justin Mason (κύριος συντηρητής του PLP) συνεργάστηκαν για να φτιάξουν το LPRng. Η κύρια τοποθεσία του LPRng είναι η http://www.lprng.org/.

CUPS

Το CUPS, ή αλλιώς Common UNIX Printing System, παρέχει μια φορητή πλατφόρμα εκτυπώσεων για λειτουργικά συστήματα βασισμένα στο UNIX®. Αναπτύχθηκε από την Easy Software

Products για να προωθήσει μια στάνταρ λύση εκτυπώσεων για όλους τους χρήστες και κατασκευαστές UNIX®.

Το CUPS χρησιμοποιεί το πρωτόκολλο Internet Printing Protocol (IPP) ως βάση του για τη διαχείριση εργασιών εκτύπωσης και ουρών αναμονής. Υποστηρίζονται επίσης, αλλά με μειωμένη λειτουργικότητα, τα πρωτόκολλα Line Printer Daemon (LPD), Server Message Block (SMB), και AppSocket (γνωστό ως JetDirect). Το CUPS προσθέτει δυνατότητες ανίχνευσης δικτυακών εκτυπωτών, ενώ μέσω των επιλογών PostScript Printer Description (PPD) γίνεται εφικτή η υποστήριξη σύγχρονων εκτυπωτών στον κόσμο του UNIX®.

Η κύρια τοποθεσία του CUPS είναι η http://www.cups.org/.

HPLIP

Το HPLIP, ή Σύστημα Απεικόνισης και Εκτύπωσης της HP για Linux®, είναι μια σουίτα εφαρμογών για συσκευές της HP, που υποστηρίζει λειτουργίες όπως η εκτύπωση, η σάρωση και η αποστολή / λήψη φαξ. Η σουίτα αυτή χρησιμοποιεί το CUPS ως backend για κάποιες από τις λειτουργίες εκτύπωσης που παρέχει.

Η κύρια δικτυακή τοποθεσία της εφαρμογής HPLIP είναι http://hplipopensource.com/hplip-web/index.html.

16.7. Εντοπισμός Βλαβών

Μετά την εκτέλεση του απλού τεστ με το lptest(1), αντί της κανονικής εκτύπωσης, μπορεί να έχετε λάβει ως αποτέλεσμα μία από τις ακόλουθες καταστάσεις:

Ο εκτυπωτής καθυστέρησε να ξεκινήσει ή δεν εκτύπωσε ολόκληρη τη σελίδα.

Ο εκτυπωτής τύπωσε το τεστ, αλλά δεν ξεκίνησε αμέσως. Ίσως χρειάστηκε να πιέσετε το πλήκτρο PRINT REMAINING ή το FORM FEED του εκτυπωτή σας για να εμφανιστεί το επιθυμητό αποτέλεσμα.

Εάν είναι όντως αυτή η περίπτωση σας, ο εκτυπωτής πιθανώς να ήταν σε αναμονή για να εξακριβώσει αν υπήρχαν πρόσθετα δεδομένα στην εργασία εκτύπωσης πριν ξεκινήσει να εκτυπώνει οτιδήποτε. Για να διορθώσετε το πρόβλημα, μπορείτε να θέσετε το φίλτρο κειμένου να στέλνει ένα χαρακτήρα FORM FEED (ή άλλο κατάλληλο) στον εκτυπωτή. Αυτό συνήθως είναι αρκετό για να μπορείτε να εκτυπώνετε κατευθείαν οποιοδήποτε κείμενο απομένει σε αναμονή στην εσωτερική μνήμη (buffer) του εκτυπωτή. Είναι επίσης χρήσιμο να ρυθμίζετε τις εκτυπώσεις σας ώστε να τελειώνουν με γεμάτη την τελευταία σελίδα, ώστε η επόμενη εργασία να μην αρχίζει από τα μισά του προηγούμενου φύλλου.

Η ακόλουθη τροποποίηση στο shell script /usr/local/libexec/if-simple εκτυπώνει ένα form feed μετά την αποστολή της εργασίας στον εκτυπωτή:

```
#!/bin/sh
#
# if-simple - Simple text input filter for lpd
# Installed in /usr/local/libexec/if-simple
#
# Simply copies stdin to stdout.  Ignores all filter arguments.
```

```
# Writes a form feed character (\f) after printing job.

/bin/cat && printf "\f" && exit 0
exit 2
```

Η εκτύπωση παρουσιάζει "φαινόμενο σκάλας (staircase effect)."

Στην εκτύπωση σας φαίνεται το ακόλουθο:

```
!"#$%&'()*+,-./01234
              "#$%&'()*+,-./012345
                            #$%&'()*+,-./0123456
```

Γίνατε ένα ακόμα θύμα του *φαινομένου σκάλας*, που προκλήθηκε από αντιφατικές ερμηνείες των χαρακτήρων με τους οποίους δηλώνεται η τροφοδοσία νέας γραμμής. Τα λειτουργικά συστήματα τύπου UNIX® χρησιμοποιούν έναν μόνο χαρακτήρα ASCII με κωδικό 10, τον line feed (τροφοδοσία γραμμής, LF). Το MS-DOS®, το OS/2®, και διάφορα άλλα, χρησιμοποιούν ένα ζεύγος χαρακτήρων ASCII κωδικού 10 *και* ASCII κωδικού 13 (τον carriage return ή αλλιώς CR). Πολλοί εκτυπωτές χρησιμοποιούν την σύμβαση του MS-DOS® για την αλλαγή γραμμής.

Όταν εκτυπώνετε με το FreeBSD, το κείμενο σας απλά χρησιμοποιεί τον χαρακτήρα τροφοδοσίας γραμμής (line feed). Ο εκτυπωτής, μόλις αντιληφθεί τον χαρακτήρα line feed, προωθεί το χαρτί κατά μία γραμμή, αλλά κρατάει την ίδια θέση οριζόντια καθώς καλείται να εκτυπώσει τον επόμενο χαρακτήρα. Σε αυτό το σημείο χρησιμοποιείται το CR (carriage return): μετακινεί δηλαδή την θέση εργασίας για τον επόμενο χαρακτήρα που πρόκειται να εκτυπωθεί στο αριστερό άκρο του χαρτιού.

Το FreeBSD επιθυμεί ο εκτυπωτής να μπορεί να ενεργεί ως εξής:

Όταν ο εκτυπωτής λαμβάνει CR	Να εκτυπώνει CR
Όταν ο εκτυπωτής λαμβάνει LF	Να εκτυπώνει CR + LF

Υπάρχουν διάφοροι τρόποι για να επιτευχθεί αυτό:

- Χρησιμοποιήστε τα πλήκτρα ρύθμισης του εκτυπωτή ή τον πίνακα ελέγχου για να αλλάξετε τον τρόπο με τον οποίο ερμηνεύει αυτούς τους χαρακτήρες ο εκτυπωτής σας. Συμβουλευτείτε το εγχειρίδιο χρήσης του για να δείτε πως μπορεί να γίνει αυτό.

Αν έχετε και άλλα λειτουργικά στο σύστημα σας εκτός από το FreeBSD, πιθανόν να χρειαστεί, όταν τα χρησιμοποιείτε, να *επαναρυθμίσετε* τον εκτυπωτή σας ώστε να ερμηνεύει διαφορετικά τους χαρακτήρες CR και LF. Στην περίπτωση αυτή, ίσως είναι καλύτερο να προτιμήσετε κάποια από τις λύσεις που ακολουθούν.

- Ο οδηγός (driver) της σειριακής γραμμής του FreeBSD μπορεί να μετατρέπει αυτόματα από LF σε CR+LF. Φυσικά, αυτό δουλεύει *μόνο* σε σειριακές θύρες. Για να ενεργοποιήσετε αυτή την λειτουργία, χρησιμοποιήστε την ικανότητα `ms#` και ορίστε την κατάσταση λειτουργίας `onlcr` στο αρχείο /etc/printcap για τον εκτυπωτή.

- Στείλτε ένα *κωδικό διαφυγής (escape code)* στον εκτυπωτή ώστε να χειρίζεται προσωρινά τους χαρακτήρες LF με διαφορετικό τρόπο. Συμβουλευτείτε το εγχειρίδιο χρήσης του εκτυπωτή σας για τους κώδικες διαφυγής που υποστηρίζονται. Όταν ανακαλύψετε τον κατάλληλο, μετατρέψτε το φίλτρο κειμένου ώστε να στέλνει πρώτα τον κωδικό, και έπειτα την εργασία στον εκτυπωτή.

  Εδώ είναι ένα παράδειγμα φίλτρου κειμένου για εκτυπωτές που καταλαβαίνουν τους κωδικούς διαφυγής PCL της Hewlett-Packard. Αυτό το φίλτρο κάνει τον εκτυπωτή να χειρίζεται τους χαρακτήρες LF ως LF και CR. Έπειτα αποστέλλει την εργασία, στέλνοντας στο τέλος της ένα χαρακτήρα αλλαγής σελίδας (form feed) ώστε να γίνει σωστή εξαγωγή της τελευταίας σελίδας. Το φίλτρο αυτό θα πρέπει να δουλεύει με σχεδόν όλους τους εκτυπωτές της Hewlett Packard.

  ```
  #!/bin/sh
  #
  # hpif - Simple text input filter for lpd for HP-PCL based printers
  # Installed in /usr/local/libexec/hpif
  #
  # Simply copies stdin to stdout.  Ignores all filter arguments.
  # Tells printer to treat LF as CR+LF.  Ejects the page when done.

  printf "\033&k2G" && cat && printf "\033&l0H" && exit 0
  exit 2
  ```

  Εδώ είναι ένα παράδειγμα για το /etc/printcap ενός υπολογιστή με όνομα `orchid`. Έχει ένα μόνο εκτυπωτή στην πρώτη παράλληλη θύρα του, ένα Hewlett Packard LaserJet 3Si με όνομα `teak`. Χρησιμοποιεί το παραπάνω script ως φίλτρο κειμένου:

  ```
  #
  #  /etc/printcap for host orchid
  #
  teak|hp|laserjet|Hewlett Packard LaserJet 3Si:\
          :lp=/dev/lpt0:sh:sd=/var/spool/lpd/teak:mx#0:\
          :if=/usr/local/libexec/hpif:
  ```

Εκτυπώνεται η μία γραμμή πάνω στην άλλη.

Ο εκτυπωτής δεν προωθεί καθόλου το χαρτί και όλες οι γραμμές κειμένου τυπώνονται η μία πάνω από την άλλη, σε μία γραμμή.

Αυτό το πρόβλημα είναι το "αντίστροφο" του φαινόμενου σκάλας, που περιγράψαμε προηγουμένως, και είναι πολύ σπάνιο. Σε κάποιο σημείο, οι χαρακτήρες LF που χρησιμοποιεί το FreeBSD για να τερματίσει την γραμμή, ερμηνεύονται ως χαρακτήρες CR οι οποίοι επιστρέφουν την κεφαλή στο αριστερό άκρο του χαρτιού, αλλά δίχως να προωθήσουν το χαρτί μία γραμμή προς τα κάτω.

Χρησιμοποιήστε τους διακόπτες ρυθμίσεων του εκτυπωτή ή τον πίνακα ελέγχου για να θέσετε τις ακόλουθες επιλογές για τα LF και CR characters:

Ο εκτυπωτής λαμβάνει	Ο εκτυπωτής τυπώνει
CR	CR
LF	CR + LF

Ο εκτυπωτής δεν εκτυπώνει (χάνει) κάποιους χαρακτήρες.

Ο εκτυπωτής, ενώ είναι σε λειτουργία εκτύπωσης, δεν εκτυπώνει κάποιους χαρακτήρες σε όλες τις γραμμές. Το πρόβλημα πιθανώς να γίνεται εντονότερο καθώς η εκτύπωση εξελίσσεται, χάνοντας ακόμη περισσότερους χαρακτήρες.

Το πρόβλημα είναι πως ο εκτυπωτής, καθώς εκτυπώνει, δεν προλαβαίνει να ακολουθήσει την ταχύτητα με την οποία ο υπολογιστής στέλνει δεδομένα μέσω της σειριακής διασύνδεσης (αυτό το πρόβλημα δεν πρέπει κανονικά να συμβαίνει σε εκτυπωτές συνδεμένους σε παράλληλες θύρες). Υπάρχουν δύο τρόποι για να ξεπεραστεί αυτό το πρόβλημα:

- Εάν ο εκτυπωτής υποστηρίζει έλεγχο ροής XON/XOFF, ρυθμίστε το FreeBSD να τον χρησιμοποιήσει ορίζοντας την κατάσταση λειτουργίας `ixon` με την ικανότητα `ms#`.
- Εάν ο εκτυπωτής υποστηρίζει έλεγχο ροής τύπου Request to Send / Clear to Send (hardware handshake, γνωστό και με την ονομασία `RTS/CTS`), πρέπει να οριστεί η κατάσταση λειτουργίας `crtscts` στην ικανότητα `ms#`. Βεβαιωθείτε πως το καλώδιο που συνδέει τον εκτυπωτή με τον υπολογιστή είναι σωστά φτιαγμένο για χρήση αυτού του ελέγχου ροής.

Ο εκτυπωτής τυπώνει σκουπίδια.

Ο εκτυπωτής τύπωσε κάτι που αποκαλούμε τυχαία σκουπίδια, εννοώντας οτιδήποτε εκτός του επιθυμητού κειμένου.

Αυτό είναι συνήθως ένα ακόμα σύμπτωμα λανθασμένων παραμέτρων σειριακής επικοινωνίας με τον εκτυπωτή. Ελέγξτε ξανά την τιμή bps rate στην ικανότητα `br`, και την ρύθμιση parity στην ικανότητα `ms#`. Βεβαιωθείτε πως ο εκτυπωτής χρησιμοποιεί τις ίδιες ρυθμίσεις που έχουν καθοριστεί στο αρχείο /etc/printcap.

Δεν συνέβη τίποτε, ο εκτυπωτής δεν ξεκίνησε καν.

Αν δεν συνέβη τίποτε, το πρόβλημα πιθανόν να οφείλεται στο FreeBSD και όχι στο hardware. Προσθέστε την ικανότητα αρχείου καταγραφής (log file, `lf`) στο αρχείο /etc/printcap, στην καταχώριση του εκτυπωτή που έχει το πρόβλημα. Για παράδειγμα, εδώ είναι η καταχώριση για τον `rattan`, με την ικανότητα `lf`:

```
rattan|line|diablo|lp|Diablo 630 Line Printer:\
        :sh:sd=/var/spool/lpd/rattan:\
        :lp=/dev/lpt0:\
        :if=/usr/local/libexec/if-simple:\
        :lf=/var/log/rattan.log
```

Έπειτα, προσπαθήστε να ξαναεκτυπώσετε. Ελέγξτε το αρχείο καταγραφής (log) (στο παράδειγμα μας, /var/log/rattan.log) για να βρείτε πιθανές αναφορές σφαλμάτων. Με βάση τα μηνύματα που βλέπετε, προσπαθήστε να διορθώσετε το πρόβλημα.

Αν δεν καθορίσετε την ικανότητα `lf`, το LPD χρησιμοποιεί από προεπιλογή το /dev/console.

Chapter 17. Συμβατότητα με Εκτελέσιμα του Linux

17.1. Σύνοψη

Το FreeBSD παρέχει binary συμβατότητα (εκτελέσιμων) με αρκετά άλλα λειτουργικά τύπου UNIX®, συμπεριλαμβανομένου και του Linux. Σε αυτό το σημείο, μπορεί να αναρωτιέστε γιατί ακριβώς χρειάζεται το FreeBSD να μπορεί να τρέξει εκτελέσιμα Linux; Η απάντηση σε αυτή την ερώτηση είναι αρκετά απλή. Πολλές εταιρίες και προγραμματιστές αναπτύσσουν εφαρμογές μόνο για Linux, μια και είναι πολύ "της μόδας" στο κόσμο των υπολογιστών. Αυτό αναγκάζει εμάς τους υπόλοιπους, που χρησιμοποιούμε το FreeBSD, να πιέζουμε τις ίδιες αυτές εταιρίες και προγραμματιστές να δημιουργήσουν κανονικές εκδόσεις των εφαρμογών τους για FreeBSD. Το πρόβλημα είναι, ότι οι περισσότερες από αυτές τις εταιρίες δεν αντιλαμβάνονται πραγματικά πόσοι περισσότεροι άνθρωποι θα χρησιμοποιούσαν το προϊόν τους αν είχαν εκδόσεις και για FreeBSD, και οι περισσότερες συνεχίζουν να αναπτύσσουν μόνο για Linux. Άρα τι μπορεί να κάνει ένας χρήστης του FreeBSD; Εδώ έρχεται να βοηθήσει η binary συμβατότητα του FreeBSD με το Linux.

Εν συντομία, η συμβατότητα επιτρέπει στους χρήστες του FreeBSD να εκτελέσουν περίπου το 90% όλων των Linux εφαρμογών χωρίς μετατροπές. Αυτό περιλαμβάνει εφαρμογές όπως το StarOffice™, την Linux έκδοση του getenv(3), Adobe® Acrobat®, RealPlayer®, Oracle®, WordPerfect®, Doom, Quake, και περισσότερα. Έχει επίσης αναφερθεί ότι σε κάποιες περιπτώσεις, τα εκτελέσιμα του Linux έχουν καλύτερη απόδοση στο FreeBSD από ότι στο Linux.

Υπάρχουν ωστόσο κάποια συγκεκριμένα για το Linux στοιχεία του λειτουργικού που δεν υποστηρίζονται στο FreeBSD. Τα εκτελέσιμα του Linux δεν θα δουλέψουν στο FreeBSD αν χρησιμοποιούν πολλές εξειδικευμένες κλήσεις i386™, όπως για παράδειγμα την ενεργοποίηση της εικονικής κατάστασης 8086.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να ενεργοποιήσετε την συμβατότητα εκτελέσιμων με το Linux στο σύστημα σας.
- Πως να εγκαταστήσετε πρόσθετες κοινόχρηστες βιβλιοθήκες του Linux.
- Πως να εγκαταστήσετε εφαρμογές του Linux στο FreeBSD.
- Τις λεπτομέρειες της υλοποίησης της συμβατότητας με το Linux στο FreeBSD.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να γνωρίζετε πως θα εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

17.2. Εγκατάσταση

Η συμβατότητα με εκτελέσιμα του Linux δεν είναι ενεργή εξ' αρχής. Ο ευκολότερος τρόπος για να ενεργοποιήσετε αυτή τη λειτουργία είναι να φορτώσετε το KLD (άρθρωμα) `linux` ("Kernel LoaDable object"). Μπορείτε να φορτώσετε αυτό το άρθρωμα στον πυρήνα δίνοντας τη παρακάτω εντολή ως `root`:

```
# kldload linux
```

Αν θέλετε να έχετε πάντα ενεργοποιημένη τη συμβατότητα με Linux, τότε θα χρειαστεί να προσθέσετε τη παρακάτω γραμμή στο /etc/rc.conf:

```
linux_enable="YES"
```

Η εντολή kldstat(8) μπορεί να χρησιμοποιηθεί για να ελεγχθεί αν το KLD είναι φορτωμένο:

```
% kldstat
Id Refs Address    Size     Name
 1    2 0xc0100000 16bdb8   kernel
 7    1 0xc24db000 d000     linux.ko
```

Αν για κάποιο λόγο δεν θέλετε ή δε μπορείτε να φορτώσετε το KLD, τότε μπορείτε να συνδέσετε στατικά την υποστήριξη εκτελέσιμων του Linux στον πυρήνα με το να προσθέσετε την επιλογή `options COMPAT_LINUX` στο αρχείων ρυθμίσεων του πυρήνα. Στη συνέχεια μπορείτε να εγκαταστήσετε τον νέο πυρήνα όπως περιγράφεται στο Ρυθμίζοντας τον Πυρήνα του FreeBSD.

17.2.1. Εγκατάσταση των Linux Runtime Libraries

Αυτό μπορεί να γίνει με δύο τρόπους. Είτε με τη χρήση του linux_base-fc4 port, ή με χειροκίνητη εγκατάσταση τους.

17.2.1.1. Εγκατάσταση μέσω του linux_base Port

Αυτός είναι κατά γενική ομολογία ο ευκολότερος τρόπος για την εγκατάσταση των runtime libraries. Είναι η ίδια διαδικασία εγκατάστασης που ακολουθείται και για οποιοδήποτε άλλο port από τη Συλλογή των Ports. Απλά κάντε το παρακάτω:

```
# cd /usr/ports/emulators/linux_base-f10
# make install distclean
```

Αν χρησιμοποιείτε κάποια έκδοση του FreeBSD πριν την 8.0, θα πρέπει να εγκαταστήσετε το port emulators/linux_base-fc4 αντί για το emulators/linux_base-f10.

Θα πρέπει τώρα να έχετε κανονική συμβατότητα με εκτελέσιμα του Linux. Μερικά προγράμματα παραπονιούνται ότι οι βιβλιοθήκες συστήματος (system libraries) δεν είναι στη τελευταία τους έκδοση. Γενικά όμως, αυτό δεν αποτελεί κανένα πρόβλημα.

Μπορούν να υπάρχουν πολλαπλές εκδόσεις του emulators/linux_base, που να αντιστοιχούν στις διαφορετικές εκδόσεις των διανομών Linux. Θα πρέπει να κάνετε εγκατάσταση των ports που προαπαιτούνται από τις εφαρμογές Linux τις

οποίες θέλετε να εγκαταστήσετε.

17.2.1.2. Χειροκίνητη εγκατάσταση των Libraries

Αν δεν έχετε εγκαταστήσει την συλλογή των "ports", μπορείτε να εγκαταστήσετε τις βιβλιοθήκες χειροκίνητα. Θα χρειαστείτε τα Linux shared libraries τα οποία απαιτεί το πρόγραμμα. Επίσης, θα χρειαστεί να δημιουργήσετε και έναν κατάλογο "shadow root", /compat/linux, για τις βιβλιοθήκες Linux που θα υπάρχουν στο FreeBSD. Οποιαδήποτε κοινές βιβλιοθήκες (shared libraries) οι οποίες χρησιμοποιούνται από εφαρμογές Linux και εκτελούνται στο FreeBSD θα κοιτάξουν πρώτα σε αυτόν τον κατάλογο. Επομένως, αν μια εφαρμογή Linux φορτώσει για παράδειγμα το /lib/libc.so, το FreeBSD θα προσπαθήσει να φορτώσει πρώτα το /compat/linux/lib/libc.so, και αν αυτό δεν υπάρχει, τότε θα προσπαθήσει να φορτώσει το /lib/libc.so. Τα shared libraries θα πρέπει να εγκατασταθούν στο shadow tree /compat/linux/lib αντί για τις τοποθεσίες που αναφέρει το `ld.so` στο Linux.

Γενικά, τουλάχιστον στις πρώτες σας εγκαταστάσεις εφαρμογών Linux, θα χρειαστεί να ψάξετε για τις κοινές βιβλιοθήκες από τα αντίστοιχα εκτελέσιμα. Μετά από κάποιο διάστημα θα έχετε ένα ικανοποιητικό αριθμό Linux shared libraries στο σύστημά σας και πλέον δε θα χρειάζεται επιπλέον εργασία πέρα από την εγκατάσταση της εφαρμογής.

17.2.1.3. Εγκατάσταση Πρόσθετων Shared Libraries

Και τι γίνεται στη περίπτωση που έχετε εγκαταστήσει το linux_base port και οι εφαρμογές σας ακόμη παραπονιούνται για shared libraries που λείπουν; Πώς μπορείτε να ξέρετε ποια shared libraries χρειάζεται κάποια εφαρμογή, και που μπορείτε να τα βρείτε; Βασικά, υπάρχουν 2 επιλογές (για να ακολουθήσετε τις παρακάτω οδηγίες θα πρέπει να είστε `root` στο σύστημά σας).

Αν έχετε πρόσβαση σε κάποιο μηχάνημα Linux, ρίξτε μια ματιά στα shared libraries που χρειάζεται μια εφαρμογή, και αντιγράψτε τα στο FreeBSD. Δείτε το παρακάτω παράδειγμα:

Ας υποθέσουμε ότι κατεβάσατε μέσω FTP το εκτελέσιμο του Doom για το Linux, και το βάλατε στο Linux σύστημα στο οποίο έχετε πρόσβαση. Μπορείτε στη συνέχεια να ελέγξετε ποια shared libraries χρειάζεται η εφαρμογή με την εντολή `ldd linuxdoom`, όπως:

```
% ldd linuxdoom
libXt.so.3 (DLL Jump 3.1) => /usr/X11/lib/libXt.so.3.1.0
libX11.so.3 (DLL Jump 3.1) => /usr/X11/lib/libX11.so.3.1.0
libc.so.4 (DLL Jump 4.5pl26) => /lib/libc.so.4.6.29
```

Θα χρειαστεί να πάρετε όλα τα αρχεία από τη τελευταία στήλη, και να τα αντιγράψετε στον κατάλογο /compat/linux, και να δημιουργήσετε προς αυτά τους αντίστοιχους συμβολικούς δεσμούς (symbolic links) με τα ονόματα της πρώτης στήλης. Αυτό σημαίνει ότι πρακτικά, θα έχετε αυτά τα αρχεία στο σύστημα σας:

```
/compat/linux/usr/X11/lib/libXt.so.3.1.0
/compat/linux/usr/X11/lib/libXt.so.3 -> libXt.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3.1.0
/compat/linux/usr/X11/lib/libX11.so.3 -> libX11.so.3.1.0
/compat/linux/lib/libc.so.4.6.29
```

```
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

Σημειώστε ότι αν έχετε ήδη κάποιο Linux shared library που ο αριθμός έκδοσης είναι ο ίδιος με αυτόν της πρώτης στήλης του `ldd`, δε θα χρειαστεί να αντιγράψετε το αρχείο όπως αυτό ονομάζεται στη τελευταία στήλη, τα υπάρχοντα αρχεία θα πρέπει να κάνουν τη δουλειά τους. Σας συμβουλεύουμε όμως να αντιγράψετε το shared library αν είναι κάποια νεότερη έκδοση. Μπορείτε να διαγράψετε τα παλιά αρχεία, αρκεί όμως να ανανεώσετε τους συμβολικούς δεσμούς ώστε να οδηγούν στα νέα αρχεία. Επομένως, αν έχετε τις παρακάτω βιβλιοθήκες στο σύστημά σας:

```
/compat/linux/lib/libc.so.4.6.27
/compat/linux/lib/libc.so.4 -> libc.so.4.6.27
```

και βρείτε μια εφαρμογή η οποία ζητάει μια νεότερη έκδοση μέσω του `ldd`:

```
libc.so.4 (DLL Jump 4.5pl26) -> libc.so.4.6.29
```

Αν η διαφορά της έκδοσης στο τελευταία ψηφίο είναι μόνο μίας ή δύο εκδόσεων, τότε μην σας απασχολεί η αντιγραφή του /lib/libc.so.4.6.29, γιατί το πρόγραμμα θα πρέπει να τρέχει κανονικά και με τη λίγο παλαιότερη έκδοση. Παρ' όλα αυτά, αν θέλετε, μπορείτε να αντικαταστήσετε το libc.so και έτσι θα έχετε το παρακάτω:

```
/compat/linux/lib/libc.so.4.6.29
/compat/linux/lib/libc.so.4 -> libc.so.4.6.29
```

Ο μηχανισμός των συμβολικών συνδέσμων χρειάζεται *μόνο* για τις εφαρμογές του Linux. Ο runtime linker του FreeBSD κοιτάει μόνος του για τις πιο πρόσφατες εκδόσεις των βιβλιοθηκών και έτσι δε χρειάζεται να σας απασχολεί.

17.2.2. Εγκατάσταση των Linux ELF Binaries

Τα ELF binaries χρειάζονται μερικές φορές ένα ακόμα βήμα, το "branding". Αν προσπαθήσετε να τρέξετε ένα εκτελέσιμο ELF χωρίς branding, τότε θα σας εμφανιστεί το παρακάτω σφάλμα:

```
% ./my-linux-elf-binary
ELF binary type not known
Abort
```

Για να βοηθήσετε τον πυρήνα του FreeBSD να ξεχωρίσει ένα ELF του FreeBSD από ένα του Linux, χρησιμοποιήστε την εντολή brandelf(1).

```
% brandelf -t Linux my-linux-elf-binary
```

Το GNU toolchain, ομάδα πρόγραμμα GNU, τοποθετεί πλέον αυτόματα τα κατάλληλα χαρακτηριστικά στα εκτελέσιμα ELF, επομένως το παραπάνω βήμα θα χρειάζεται όλο και λιγότερο στο μέλλον.

17.2.3. Εγκατάσταση μιας Τυχαίας Linux RPM Εφαρμογής

Το FreeBSD διαθέτει την δική του βάση δεδομένων για τα πακέτα, η οποία χρησιμοποιείται για όλα τα ports (και για αυτά που προέρχονται από το Linux®). Για το λόγο αυτό, η βάση δεδομένων Linux® RPM δεν χρησιμοποιείται (δεν υποστηρίζεται).

Αν ωστόσο χρειάζεται να εγκαταστήσετε μια οποιαδήποτε εφαρμογή του Linux® που βασίζεται σε πακέτο RPM, μπορείτε να το επιτύχετε με τον παρακάτω τρόπο:

```
# cd /compat/linux
# rpm2cpio -q < /path/to/linux.archive.rpm | cpio -id
```

Χρησιμοποιήστε την brandelf(1) για να τυποποιήσετε κατάλληλα τα εκτελέσιμα (όχι τις βιβλιοθήκες!) ως εφαρμογές Linux®. Δεν θα μπορείτε να απεγκαταστήσετε τις εφαρμογές με καθαρό τρόπο, αλλά θα μπορέσετε να κάνετε τις δοκιμές που επιθυμείτε.

17.2.4. Ρύθμιση του Hostname Resolver

Αν το DNS δε δουλεύει ή αν σας εμφανίζεται το παρακάτω σφάλμα:

```
resolv+: "bind" is an invalid keyword resolv+:
"hosts" is an invalid keyword
```

Θα χρειαστεί να ρυθμίσετε το /compat/linux/etc/host.conf ώστε να περιέχει:

```
order hosts, bind
multi on
```

Η σειρά εδώ δηλώνει ότι αρχικά ελέγχεται το αρχείο /etc/hosts και στη συνέχεια ο DNS server. Όταν το /compat/linux/etc/host.conf δεν είναι διαθέσιμο, οι εφαρμογές Linux χρησιμοποιούν το /etc/host.conf του FreeBSD και παραπονιούνται ότι η σύνταξη του αρχείου δεν είναι σωστή. Θα πρέπει να αφαιρέσετε την αναφορά στο `bind` αν δεν έχετε ρυθμίσει ένα name server μέσω του /etc/resolv.conf.

17.3. Εγκαθιστώντας το Mathematica®

Το κείμενο αυτό περιγράφει τη διαδικασία εγκατάστασης της έκδοσης Linux του Mathematica® 5.X σε ένα σύστημα FreeBSD.

Μπορείτε να αγοράσετε την κανονική ή μαθητική έκδοση του Mathematica® για Linux, απευθείας από τη Wolfram στο http://www.wolfram.com/.

17.3.1. Το Πρόγραμμα Εγκατάστασης του Mathematica®

Αρχικά, θα πρέπει να πείτε στο FreeBSD ότι τα εκτελέσιμα για Linux του Mathematica® κάνουν χρήση του Linux ABI. Ο ευκολότερος τρόπος για να το κάνετε αυτό είναι να ορίσετε τον τύπο του ELF ως Linux σε όλες τις εφαρμογές που δεν είναι ήδη branded, κάνοντας χρήση της εντολής:

```
# sysctl kern.fallback_elf_brand=3
```

Αυτό θα κάνει το FreeBSD να υποθέσει ότι τα εκτελέσιμα ELF που δεν είναι branded, κάνουν χρήση του Linux ABI και έτσι θα μπορείτε να τρέξετε το πρόγραμμα της εγκατάστασης απευθείας από το CDROM.

Τώρα, αντιγράψτε το αρχείο MathInstaller στον σκληρό σας δίσκο:

```
# mount /cdrom
# cp /cdrom/Unix/Installers/Linux/MathInstaller /localdir/
```

Ανοίξτε το αρχείο και αντικαταστήστε το `/bin/sh` στη πρώτη γραμμή με το `/compat/linux/bin/sh`. Αυτό θα σιγουρέψει ότι το πρόγραμμα εγκατάστασης θα τρέχει με την έκδοση sh(1) για Linux. Στη συνέχεια, αντικαταστήστε όλες τις εγγραφές `Linux)` με `FreeBSD)` χρησιμοποιώντας έναν συντάκτη κειμένου ή με το παρακάτω script στην επόμενη ενότητα. Αυτό θα πει στο πρόγραμμα εγκατάστασης του Mathematica®, το οποίο τρέχει την εντολή `uname -s` για να διαπιστώσει το λειτουργικό σύστημα, να αντιμετωπίσει το FreeBSD σαν ένα λειτουργικό παρεμφερές με το Linux. Η εκτέλεση του `MathInstaller` θα ξεκινήσει τώρα την εγκατάσταση του Mathematica®.

17.3.2. Τροποποιώντας τα Εκτελέσιμα του Mathematica®

Τα shell scripts τα οποία δημιουργεί το Mathematica® κατά τη διαδικασία της εγκατάστασης πρέπει να τροποποιηθούν πριν χρησιμοποιηθούν. Αν επιλέξετε το /usr/local/bin ως τον κατάλογο για τα εκτελέσιμα του Mathematica®, θα βρείτε εκεί συμβολικούς δεσμούς (symlinks) προς τα αρχεία math, mathematica, Mathematica, και MathKernel. Σε κάθε περίπτωση από τις παραπάνω, αντικαταστήστε τις εγγραφές `Linux)` με `FreeBSD)` με κάποιον συντάκτη κειμένου ή με το παρακάτω shell script:

```
#!/bin/sh
cd /usr/local/bin
for i in math mathematica Mathematica MathKernel
  do sed 's/Linux)/FreeBSD)/g' $i > $i.tmp
  sed 's/\/bin\/sh/\/compat\/linux\/bin\/sh/g' $i.tmp > $i
  rm $i.tmp
  chmod a+x $i
done
```

17.3.3. Αποκτώντας Κωδικό για το Mathematica®

Όταν εκκινήσετε το Mathematica® για πρώτη φορά, θα ερωτηθείτε για έναν κωδικό. Αν δεν έχετε

κάποιον κωδικό σε αυτό το στάδιο, τρέξτε το πρόγραμμα `mathinfo` που βρίσκεται στον κατάλογο εγκατάστασης για να σας δοθεί το "machine ID". Το "machine ID" είναι εξ' ολοκλήρου βασισμένο στη διεύθυνση MAC της κάρτας δικτύου που έχετε. Αυτό σημαίνει ότι δεν μπορείτε να τρέξετε το Mathematica® σε άλλους υπολογιστές.

Όταν εγγραφείτε στη Wolfram, με e-mail, τηλέφωνο ή fax, θα χρειαστεί να δώσετε το "machine ID" και θα σας απαντήσουν με έναν αντίστοιχο κωδικό που θα αποτελείται από μια σειρά αριθμών.

17.3.4. Τρέχοντας το Mathematica® Frontend μέσω Δικτύου

Το Mathematica® κάνει χρήση κάποιων ειδικών γραμματοσειρών για να εμφανίσει χαρακτήρες οι οποίοι δεν υπάρχουν στα συνηθισμένα σετ (ολοκληρώματα, αθροίσματα, Ελληνικά γράμματα, κλπ). Το πρωτόκολλο X απαιτεί αυτές οι γραμματοσειρές να υπάρχουν στο *τοπικό* σύστημα. Αυτό σημαίνει ότι θα χρειαστεί να αντιγράψετε τις γραμματοσειρές αυτές από το CDROM ή από από κάποιον άλλον υπολογιστή που έχει το Mathematica®. Συνήθως αυτές οι γραμματοσειρές μπορούν να βρεθούν μέσα στο κατάλογο /cdrom/Unix/Files/SystemFiles/Fonts του CDROM, ή στον κατάλογο /usr/local/mathematica/SystemFiles/Fonts στον τοπικό σκληρό δίσκο. Οι πραγματικές γραμματοσειρές βρίσκονται σε υποκαταλόγους όπως Type1 και X. Υπάρχουν αρκετοί τρόποι να τις χρησιμοποιήσετε, οι οποίοι περιγράφονται στη συνέχεια.

Ο πρώτος τρόπος είναι να τις αντιγράψετε μέσα σε έναν υπάρχοντα κατάλογο στο /usr/X11R6/lib/X11/fonts. Θα χρειαστεί όμως να τροποποιήσετε το αρχείο fonts.dir, ώστε να προσθέσετε τα ονόματα των γραμματοσειρών μέσα σε αυτό, και να αλλάξετε τον αριθμό των γραμματοσειρών στη πρώτη γραμμή. Εναλλακτικά, είναι συνήθως αρκετό να εκτελέσετε απλώς την εντολή mkfontdir(1) μέσα στον κατάλογο που έχετε αντιγράψει τις γραμματοσειρές.

Ο δεύτερος τρόπος είναι να αντιγράψετε τους παραπάνω καταλόγους μέσα στο /usr/X11R6/lib/X11/fonts:

```
# cd /usr/X11R6/lib/X11/fonts
# mkdir X
# mkdir MathType1
# cd /cdrom/Unix/Files/SystemFiles/Fonts
# cp X/* /usr/X11R6/lib/X11/fonts/X
# cp Type1/* /usr/X11R6/lib/X11/fonts/MathType1
# cd /usr/X11R6/lib/X11/fonts/X
# mkfontdir
# cd ../MathType1
# mkfontdir
```

Τώρα προσθέστε τους νέους καταλόγους με τις γραμματοσειρές στο font path:

```
# xset fp+ /usr/X11R6/lib/X11/fonts/X
# xset fp+ /usr/X11R6/lib/X11/fonts/MathType1
# xset fp rehash
```

Αν χρησιμοποιείτε το Xorg, μπορείτε να φορτώνετε τις γραμματοσειρές αυτές αυτόματα,

προσθέτοντας τους νέους καταλόγους στο αρχείο xorg.conf.

Αν *δεν* έχετε ήδη έναν κατάλογο με το όνομα /usr/X11R6/lib/X11/fonts/Type1, μπορείτε να αλλάξετε το όνομα του MathType1 από το παραπάνω παράδειγμα σε Type1.

17.4. Εγκαθιστώντας το Maple™

Το Maple™ είναι μία εμπορική εφαρμογή μαθηματικών παρόμοια με το Mathematica®. Θα πρέπει να αγοράσετε το λογισμικό από το http://www.maplesoft.com/ και στη συνέχεια να κάνετε αίτηση για μια άδεια χρήσης. Για να εγκαταστήσετε το λογισμικό στο FreeBSD, ακολουθήστε τα παρακάτω απλά βήματα.

1. Εκτελέστε το INSTALL shell script από το μέσο εγκατάστασης που έχετε. Επιλέξτε "RedHat" όταν ερωτηθείτε από το πρόγραμμα εγκατάστασης. Ο τυπικός κατάλογος είναι ο /usr/local/maple.
2. Αν δεν έχετε αγοράσει ακόμη κάποια άδεια για το Maple™, αγοράστε μία από το Maple Waterloo Software (http://register.maplesoft.com/) και αντιγράψτε το αρχείο που θα σας δοθεί στο /usr/local/maple/license/license.dat.
3. Εγκαταστήσετε το FLEXlm license manager εκτελώντας το INSTALL_LIC shell script το οποία παρέχεται μαζί με το Maple™. Δώστε το βασικό όνομα του υπολογιστή σας το οποίο απαιτείται από τον εξυπηρετητή διαχείρισης των αδειών (license server).
4. Χρησιμοποιήστε το παρακάτω patch στο αρχείο /usr/local/maple/bin/maple.system.type:

```
   ----- snip ------------------
*** maple.system.type.orig      Sun Jul  8 16:35:33 2001
--- maple.system.type   Sun Jul  8 16:35:51 2001
***************
*** 72,77 ****
--- 72,78 ----
          # the IBM RS/6000 AIX case
          MAPLE_BIN="bin.IBM_RISC_UNIX"
          ;;
+     "FreeBSD"|\
      "Linux")
          # the Linux/x86 case
        # We have two Linux implementations, one for Red Hat and
   ----- snip end of patch -----
```

   Σημειώστε ότι μετά το `"FreeBSD"|\` δεν πρέπει να εμφανίζεται άλλο κενό διάστημα.

   Το patch αυτό οδηγεί το Maple™ να αναγνωρίσει το "FreeBSD" σαν ένα σύστημα Linux. Το bin/maple shell script καλεί το bin/maple.system.type shell script, το οποίο με τη σειρά του καλεί την εντολή `uname -a` προκειμένου να εντοπιστεί το όνομα του λειτουργικού συστήματος. Αναλόγως με το ποιο λειτουργικό βρεθεί, θα χρησιμοποιηθούν και τα αντίστοιχα εκτελέσιμα αρχεία.

5. Εκκινήστε τον license server.

Ένας βολικός τρόπος για να εκκινήσετε το `lmgrd` είναι το ακόλουθο script που βρίσκεται στο /usr/local/etc/rc.d/lmgrd.sh:

```
   ----- snip ------------

#! /bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin
PATH=${PATH}:/usr/local/maple/bin:/usr/local/maple/FLEXlm/UNIX/LINUX
export PATH

LICENSE_FILE=/usr/local/maple/license/license.dat
LOG=/var/log/lmgrd.log

case "$1" in
start)
    lmgrd -c ${LICENSE_FILE} 2>> ${LOG} 1>&2
    echo -n " lmgrd"
    ;;
stop)
    lmgrd -c ${LICENSE_FILE} -x lmdown 2>> ${LOG} 1>&2
    ;;
*)
    echo "Usage: `basename $0` {start|stop}" 1>&2
    exit 64
    ;;
esac

exit 0
   ----- snip ------------
```

6. Δοκιμή του Maple™:

```
% cd /usr/local/maple/bin
% ./xmaple
```

Σε αυτό το σημείο θα πρέπει να είναι όλα έτοιμα και να μην έχετε κανένα πρόβλημα. Μην ξεχάσετε όμως να στείλετε ένα e-mail στη Maplesoft και να τους πείτε ότι θέλετε μια έκδοση που να υποστηρίζεται επίσημα στο FreeBSD.

17.4.1. Συνηθισμένα Προβλήματα

- Ίσως δυσκολευτείτε με την λειτουργία του FLEXlm license manager. Επιπλέον τεκμηρίωση μπορείτε να βρείτε στο http://www.globetrotter.com/.
- Το `lmgrd` είναι γνωστό ότι θέλει το αρχείο της άδειας να έχει συγκεκριμένη μορφή αλλιώς η εκτέλεση του θα αποτύχει. Ένα σωστό αρχείο άδειας χρήσης πρέπει είναι σε γενικές γραμμές όπως το παρακάτω:

```
# ====================================================
# License File for UNIX Installations ("Pointer File")
# ====================================================
SERVER chillig ANY
#USE_SERVER
VENDOR maplelmg

FEATURE Maple maplelmg 2000.0831 permanent 1 XXXXXXXXXXX \
         PLATFORMS=i86_r ISSUER="Waterloo Maple Inc." \
         ISSUED=11-may-2000 NOTICE=" Technische Universitat Wien" \
         SN=XXXXXXXXX
```

Ο σειριακός αριθμός και το κλειδί φαίνονται εδώ με 'X'. Το `chillig` είναι το όνομα του συστήματος.

Μπορείτε να τροποποιήσετε το αρχείο της άδειας χρήσης, αρκεί να μην αλλάξετε την γραμμή "FEATURE" (η οποία προστατεύεται από το κλειδί της άδειας).

17.5. Εγκαθιστώντας το MATLAB®

Το κείμενο αυτό περιγράφει τη διαδικασία εγκατάστασης της Linux έκδοσης του MATLAB® 6.5 σε ένα σύστημα FreeBSD. Δουλεύει αρκετά καλά, με εξαίρεση το Java Virtual Machine™ (δείτε στο Σύνδεση με το Περιβάλλον του Java™ Runtime Environment).

Η Linux έκδοση του MATLAB® μπορεί να αγοραστεί απευθείας από την εταιρεία The MathWorks στο http://www.mathworks.com. Σιγουρευτείτε ότι πήρατε και το αρχείο που περιέχει την άδεια χρήσης ή οδηγίες για το πως να το δημιουργήσετε. Μια και θα επικοινωνήσετε με την εταιρεία, πείτε τους ότι θα θέλατε να υπάρχει επίσης υποστήριξη για το FreeBSD.

17.5.1. Εγκατάσταση του MATLAB®

Για να εγκαταστήσετε το MATLAB®, κάντε τα παρακάτω:

1. Εισάγετε το CD και προσαρτήστε το στο σύστημα σας. Συνδεθείτε ως χρήστης `root`, όπως συνιστά το script της εγκατάστασης. Για να ξεκινήσετε το script της εγκατάστασης δώστε την εντολή:

```
# /compat/linux/bin/sh /cdrom/install
```

Το πρόγραμμα της εγκατάστασης είναι σε γραφικό περιβάλλον. Αν λαμβάνετε σφάλματα σχετικά με την οθόνη, δώστε την εντολή: `setenv HOME ~USER`, όπου *USER* είναι ο χρήστης από όπου δώσατε την εντολή su(1).

2. Όταν ερωτηθείτε για τον κατάλογο του MATLAB®, δώστε: `/compat/linux/usr/local/matlab`.

Για ευκολότερη διαδικασία εγκατάστασης, ορίστε το παρακάτω: `set`

`MATLAB=/compat/linux/usr/local/matlab` στη γραμμή εντολών του κελύφους σας.

3. Τροποποιήσετε το αρχείο της άδειας (license file) σύμφωνα με τις οδηγίες που λάβατε με την άδεια του MATLAB®.

Μπορείτε να ετοιμάσετε εκ των προτέρων το αρχείο αυτό και να το αντιγράψετε στο $MATLAB/license.dat, πριν καν σας πει το πρόγραμμα εγκατάστασης να το τροποποιήσετε.

4. Ολοκλήρωση της Εγκατάστασης

Σε αυτό το σημείο, η εγκατάσταση του MATLAB® έχει ολοκληρωθεί. Τα επόμενα βήματα χρειάζονται για να μπορέσετε να το δουλέψετε σωστά με το FreeBSD.

17.5.2. Εκκίνηση του License Manager

1. Δημιουργία συμβολικών συνδέσμων για τα scripts του license manager:

```
# ln -s $MATLAB/etc/lmboot /usr/local/etc/lmboot_TMW
# ln -s $MATLAB/etc/lmdown /usr/local/etc/lmdown_TMW
```

2. Δημιουργήστε το αρχείο εκκίνησης /usr/local/etc/rc.d/flexlm.sh. Το παράδειγμα παρακάτω είναι μια τροποποιημένη έκδοση του $MATLAB/etc/rc.lm.glnx86. Οι αλλαγές είναι στις τοποθεσίες των αρχείων, και στην εκκίνηση του license manager στο περιβάλλον εξομοίωσης Linux του FreeBSD .

```
#!/bin/sh
case "$1" in
  start)
        if [ -f /usr/local/etc/lmboot_TMW ]; then
              /compat/linux/bin/sh /usr/local/etc/lmboot_TMW -u username && echo
'MATLAB_lmgrd'
        fi
        ;;
  stop)
    if [ -f /usr/local/etc/lmdown_TMW ]; then
            /compat/linux/bin/sh /usr/local/etc/lmdown_TMW  > /dev/null 2>&1
    fi
        ;;
  *)
    echo "Usage: $0 {start|stop}"
    exit 1
    ;;
esac

exit 0
```

Το αρχείο πρέπει να είναι εκτελέσιμο:

```
# chmod +x /usr/local/etc/rc.d/flexlm.sh
```

Πρέπει επίσης να αντικαταστήσετε το παραπάνω *username* με ένα υπαρκτό όνομα χρήστη του συστήματος σας (και να μην είναι ο `root`).

3. Εκκινήστε τον license manager με την εντολή:

```
# /usr/local/etc/rc.d/flexlm.sh start
```

17.5.3. Σύνδεση με το Περιβάλλον του Java™ Runtime Environment

Αλλάξτε τον σύνδεσμο τουJava™ Runtime Environment (JRE) σε έναν ο οποίος θα δουλεύει στο FreeBSD:

```
# cd $MATLAB/sys/java/jre/glnx86/
# unlink jre; ln -s ./jre1.1.8 ./jre
```

17.5.4. Δημιουργήστε το Script Εκκίνησης του MATLAB®

1. Τοποθετήστε το παρακάτω script στο /usr/local/bin/matlab:

```
#!/bin/sh
/compat/linux/bin/sh /compat/linux/usr/local/matlab/bin/matlab "$@"
```

2. Στη συνέχεια δώστε την εντολή `chmod +x /usr/local/bin/matlab`.

Ανάλογα με την έκδοση του emulators/linux_base, που έχετε, μπορεί να εμφανιστούν μερικά σφάλματα όταν τρέξετε το script. Για να το αποφύγετε αυτό, τροποποιήστε το αρχείο /compat/linux/usr/local/matlab/bin/matlab, και αλλάξτε τη γραμμή που λέει:

```
if [ `expr "$lscmd" : '.*->.*'` -ne 0 ]; then
```

(στην έκδοση 13.0.1 βρίσκεται στη γραμμή 410) σε αυτή τη γραμμή:

```
if test -L $newbase; then
```

17.5.5. Δημιουργία Script Τερματισμού του MATLAB®

Τα επόμενα βήματα χρειάζονται για να λύσετε ένα πρόβλημα που υπάρχει με τον τερματισμό του

MATLAB®.

1. Δημιουργήστε το αρχείο $MATLAB/toolbox/local/finish.m, και μέσα σε αυτό προσθέστε μόνο τη γραμμή:

```
! $MATLAB/bin/finish.sh
```

Το $MATLAB γράψτε το ακριβώς όπως το βλέπετε.

Στον ίδιο κατάλογο, θα βρείτε τα αρχεία finishsav.m και finishdlg.m, τα οποία θα σας δίνουν τη δυνατότητα να σώζετε την εργασία σας πριν κλείσετε το πρόγραμμα. Αν πρόκειται να χρησιμοποιήσετε κάποιο από αυτά, προσθέστε του την παραπάνω γραμμή αμέσως μετά την εντολή save .

2. Δημιουργήστε το αρχείο $MATLAB/bin/finish.sh, το οποίο θα περιέχει τα παρακάτω:

```
#!/compat/linux/bin/sh
(sleep 5; killall -1 matlab_helper) &
exit 0
```

3. Κάντε το αρχείο εκτελέσιμο:

```
# chmod +x $MATLAB/bin/finish.sh
```

17.5.6. Χρησιμοποιώντας το MATLAB®

Σε αυτό το σημείο θα πρέπει να είστε έτοιμοι να δώσετε την εντολή matlab και να αρχίσετε να χρησιμοποιείτε την εφαρμογή.

17.6. Εγκατάσταση της Oracle®

17.6.1. Εισαγωγή

Το κείμενο αυτό περιγράφει τη διαδικασία εγκατάστασης των Oracle® 8.0.5 και Oracle® 8.0.5.1 Enterprise Edition για Linux σε ένα σύστημα FreeBSD.

17.6.2. Εγκατάσταση του Περιβάλλοντος Linux

Σιγουρευτείτε ότι έχετε εγκαταστήσει τα emulators/linux_base και devel/linux_devtools από τη συλλογή των Ports. Αν αντιμετωπίζετε δυσκολίες με τα παραπάνω, ίσως χρειαστεί να τα εγκαταστήσετε από πακέτα ή από παλιότερες εκδόσεις της συλλογής των Ports.

Αν θέλετε να τρέξετε τον intelligent agent, θα χρειαστεί να εγκαταστήσετε και το πακέτο Red Hat Tcl: tcl-8.0.3-20.i386.rpm. Η εντολή για την εγκατάσταση μέσω του επίσημου RPM port (archivers/rpm) είναι:

```
# rpm -i --ignoreos --root /compat/linux --dbpath /var/lib/rpm package
```

Η εγκατάσταση του *package* θα πρέπει να γίνει ομαλά και χωρίς προβλήματα.

17.6.3. Ρυθμίζοντας το Περιβάλλον για την Oracle®

Πριν την εγκατάσταση της Oracle®, θα πρέπει να ρυθμίσετε σωστά το περιβάλλον του συστήματός σας. Το παρακάτω κείμενο περιγράφει τι *ακριβώς* πρέπει να κάνετε για να εκτελέσετε την Oracle® για Linux στο FreeBSD, και δεν περιγράφει ότι υπάρχει ήδη στον οδηγό εγκατάστασης της Oracle®.

17.6.3.1. Ρύθμιση του Πυρήνα

Όπως περιγράφει ο οδηγός εγκατάστασης της Oracle®, θα πρέπει να ορίσετε τις τιμές της shared memory στο μέγιστο. Μην χρησιμοποιήσετε το `SHMMAX` στο FreeBSD. Το `SHMMAX` υπολογίζεται απλώς από το `SHMMAXPGS` και το `PGSIZE`. Επομένως καθορίστε το `SHMMAXPGS`. Όλες οι άλλες επιλογές μπορούν να οριστούν όπως περιγράφεται στον οδηγό. Για παράδειγμα:

```
options SHMMAXPGS=10000
options SHMMNI=100
options SHMSEG=10
options SEMMNS=200
options SEMMNI=70
options SEMMSL=61
```

Ορίστε τις τιμές των επιλογών έτσι ώστε να ταιριάζουν στη χρήση της Oracle® που θέλετε να κάνετε.

Επίσης, επιβεβαιώστε ότι έχετε ενεργοποιήσει τις παρακάτω επιλογές στις ρυθμίσεις του πυρήνα:

```
options SYSVSHM #SysV shared memory
options SYSVSEM #SysV semaphores
options SYSVMSG #SysV interprocess communication
```

17.6.3.2. Ο Χρήστης Oracle®

Δημιουργήστε ένα χρήστη συστήματος με όνομα `oracle`, με τον ίδιο τρόπο που θα δημιουργούσατε και οποιονδήποτε άλλον χρήστη. Το μόνο ιδιαίτερο χαρακτηριστικό του χρήστη `oracle` είναι ότι χρειάζεται να του δώσετε ένα κέλυφος Linux. Προσθέστε το `/compat/linux/bin/bash` στο /etc/shells και ορίστε το κέλυφος του χρήστη `oracle` σε /compat/linux/bin/bash.

17.6.3.3. Το Περιβάλλον

Εκτός των συνηθισμένων μεταβλητών της Oracle®, όπως οι `ORACLE_HOME` και `ORACLE_SID` θα πρέπει να ορίσετε και τις ακόλουθες μεταβλητές περιβάλλοντος:

Μεταβλητή	Τιμή
LD_LIBRARY_PATH	$ORACLE_HOME/lib
CLASSPATH	$ORACLE_HOME/jdbc/lib/classes111.zip
PATH	/compat/linux/bin /compat/linux/sbin /compat/linux/usr/bin /compat/linux/usr/sbin /bin /sbin /usr/bin /usr/sbin /usr/local/bin $ORACLE_HOME/bin

Σας συνιστούμε να ορίσετε όλες τις μεταβλητές περιβάλλοντος στο αρχείο .profile. Ένα ολοκληρωμένο παράδειγμα είναι το παρακάτω:

```
ORACLE_BASE=/oracle; export ORACLE_BASE
ORACLE_HOME=/oracle; export ORACLE_HOME
LD_LIBRARY_PATH=$ORACLE_HOME/lib
export LD_LIBRARY_PATH
ORACLE_SID=ORCL; export ORACLE_SID
ORACLE_TERM=386x; export ORACLE_TERM
CLASSPATH=$ORACLE_HOME/jdbc/lib/classes111.zip
export CLASSPATH
PATH=/compat/linux/bin:/compat/linux/sbin:/compat/linux/usr/bin
PATH=$PATH:/compat/linux/usr/sbin:/bin:/sbin:/usr/bin:/usr/sbin
PATH=$PATH:/usr/local/bin:$ORACLE_HOME/bin
export PATH
```

17.6.4. Εγκατάσταση της Oracle®

Λόγω μια μικρής έλλειψης στον εξομοιωτή του Linux, θα χρειαστεί να δημιουργήσετε έναν κατάλογο με το όνομα .oracle μέσα στο /var/tmp, πριν ξεκινήσετε το πρόγραμμα εγκατάστασης. Ο κατάλογος αυτός θα πρέπει να ανήκει στον χρήστη `oracle`. Θα πρέπει τώρα να πραγματοποιήσετε την εγκατάσταση της Oracle® δίχως κανένα πρόβλημα. Αν αντιμετωπίζετε όμως ακόμη προβλήματα, ελέγξτε την έκδοση της Oracle® που έχετε ή/και τις ρυθμίσεις σας! Αφότου έχετε πραγματοποιήσει την εγκατάσταση της Oracle®, εφαρμόστε τα patches που περιγράφονται στις δύο παρακάτω ενότητες.

Ένα συχνό πρόβλημα είναι ότι δεν γίνεται σωστή εγκατάσταση του προσαρμογέα του πρωτοκόλλου TCP. Αυτό έχει ως αποτέλεσμα να μην μπορείτε να ξεκινήσετε τους TCP listeners. Οι ακόλουθες οδηγίες θα σας βοηθήσουν να λύσετε αυτό το πρόβλημα.:

```
# cd $ORACLE_HOME/network/lib
# make -f ins_network.mk ntcontab.o
# cd $ORACLE_HOME/lib
# ar r libnetwork.a ntcontab.o
# cd $ORACLE_HOME/network/lib
# make -f ins_network.mk install
```

Μη ξεχάσετε να τρέξετε ξανά το root.sh

17.6.4.1. Διόρθωση του root.sh

Όταν εγκαθιστάτε την Oracle®, κάποιες ενέργειες, οι οποίες χρειάζονται να γίνουν ως `root`, καταγράφονται σε ένα shell script που λέγεται root.sh. Το script αυτό δημιουργείται στον κατάλογο orainst. Εφαρμόστε το παρακάτω patch στο root.sh, για να μπορέσει να βρει και να χρησιμοποιήσει το `chown`. Εναλλακτικά, τρέξτε το script μέσα από ένα κέλυφος Linux.

```
*** orainst/root.sh.orig Tue Oct 6 21:57:33 1998
--- orainst/root.sh Mon Dec 28 15:58:53 1998
***************
*** 31,37 ****
# This is the default value for CHOWN
# It will redefined later in this script for those ports
# which have it conditionally defined in ss_install.h
! CHOWN=/bin/chown
#
# Define variables to be used in this script
--- 31,37 ----
# This is the default value for CHOWN
# It will redefined later in this script for those ports
# which have it conditionally defined in ss_install.h
! CHOWN=/usr/sbin/chown
#
# Define variables to be used in this script
```

Όταν δεν κάνετε χρήση του CD για την εγκατάσταση, μπορείτε να περάσετε το patch για το root.sh, στην πηγή εγκατάστασης. Το αρχείο ονομάζεται rthd.sh και βρίσκεται στον κατάλογο orainst.

17.6.4.2. Διόρθωση του genclntsh

Το script `genclntsh` χρησιμοποιείται για να δημιουργήσει μια shared client library. Τρέξτε το παρακάτω patch για να σβήσετε το καθορισμένο `PATH`:

```
*** bin/genclntsh.orig Wed Sep 30 07:37:19 1998
--- bin/genclntsh Tue Dec 22 15:36:49 1998
***************
*** 32,38 ****
#
# Explicit path to ensure that we're using the correct commands
#PATH=/usr/bin:/usr/ccs/bin export PATH
! PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin export PATH
#
# each product MUST provide a $PRODUCT/admin/shrept.lst
--- 32,38 ----
#
# Explicit path to ensure that we're using the correct commands
#PATH=/usr/bin:/usr/ccs/bin export PATH
! #PATH=/usr/local/bin:/bin:/usr/bin:/usr/X11R6/bin export PATH
#
```

```
# each product MUST provide a $PRODUCT/admin/shrept.lst
```

17.6.5. Εκτέλεση της Oracle®

Αφού έχετε ακολουθήσει αυτές τις οδηγίες, θα πρέπει να μπορείτε να εκτελέσετε την Oracle® σαν να βρισκόσασταν σε ένα σύστημα Linux.

17.7. Προχωρημένα Θέματα

Αν έχετε την απορία πως λειτουργεί η συμβατότητα με εφαρμογές Linux, τότε θα πρέπει να διαβάσετε τη παρακάτω ενότητα. Τα περισσότερα από όσα έχουν γραφτεί είναι βασισμένα στην ηλεκτρονική λίστα γενικών συζητήσεων του FreeBSD και έχουν γραφτεί από τον Terry Lambert tlambert@primenet.com (Message ID: <199906020108.SAA07001@usr09.primenet.com>).

17.7.1. Πως Λειτουργεί;

Το FreeBSD περιέχει ένα επίπεδο αφαίρεσης (abstraction) που ονομάζεται "execution class loader". Αυτό βασίζεται στο execve(2).

Αυτό που συμβαίνει είναι ότι το FreeBSD έχει μια λίστα φορτωτών (loaders), αντί για ένα που να καταφεύγει σε περίπτωση αποτυχίας στο `#!` για να τρέξει κάποιο shell interpreter ή shell script.

Ιστορικά, ο μόνος φορτωτής στη πλατφόρμα του UNIX® έλεγχε τον μαγικό αριθμό (γενικά τα πρώτα 4 ή 8 bytes του αρχείου) για να δει αν είναι κάποιο εκτελέσιμο / εφαρμογή γνωστό στο σύστημα, και στην περίπτωση αυτή να καλέσει τον αντίστοιχο φορτωτή.

Αν το αρχείο δεν ήταν εκτελέσιμο με βάση τον τύπο του συστήματος, η κλήση στο execve(2) επέστρεφε κάποιο σφάλμα, και το shell προσπαθούσε να εκτελέσει το αρχείο σαν shell script.

Η γενική ιδέα ήταν "αν δεν είναι εκτελέσιμο, προσπάθησε να το τρέξεις ως shell script με βάση το τρέχον shell ".

Αργότερα, βρέθηκε ένας έξυπνος τρόπος ώστε το sh(1) να ελέγχει τους πρώτους δύο χαρακτήρες, και αν ήταν `:\n`, τότε καλούσε το shell csh(1) (πιστεύουμε πως η λύση αυτή βρέθηκε αρχικά από τη SCO).

Αυτό που κάνει τώρα το FreeBSD είναι να διατρέχει τη λίστα με όλους τους φορτωτές, με ένα γενικό φορτωτή `#!` ο οποίος αναγνωρίζει ως διερμηνέα (interpreter) τους χαρακτήρες από το επόμενο κενό μετά το `!` και μέχρι το τέλος, ενώ αν δεν αναγνωριστεί κάποιος, χρησιμοποιείται ως έσχατη λύση το /bin/sh.

Για την υποστήριξη του Linux ABI, το FreeBSD βλέπει τον μαγικό αριθμό του ELF binary (δε αναγνωρίζει τη διαφορά ανάμεσα σε FreeBSD, Solaris™, Linux, ή κάποιο άλλο λειτουργικό σύστημα το οποίο χρησιμοποιεί αρχεία τύπου ELF).

Ο φορτωτής ELF κοιτάει για ένα ειδικό *brand*, το οποίο είναι μια ενότητα σχολίων μέσα στο ELF image, και το οποίο δεν υπάρχει σε ELF binaries για SVR4/Solaris™

Για να λειτουργήσουν τα εκτελέσιμα του Linux, θα πρέπει να γίνουν *branded* (μαρκαριστούν) ως

Linux μέσω της brandelf(1):

```
# brandelf -t Linux file
```

Όταν γίνει αυτό, ο φορτωτής ELF θα βλέπει το Linux brand πάνω στο αρχείο.

Όταν ο φορτωτής ELF δει το Linux brand, θα αντικαταστήσει έναν δείκτη μέσα στη δομή proc. Όλες οι κλήσεις του συστήματος ταξινομούνται μέσα από αυτόν τον δείκτη (σε ένα παραδοσιακό σύστημα UNIX®, ο δείκτης θα ήταν ο πίνακας sysent[], που περιέχει τις κλήσεις του συστήματος (system calls)). Επιπλέον, η διεργασία σημειώνεται για ειδική μεταχείριση του trap vector και άλλες (μικρές) διορθώσεις, τις οποίες χειρίζεται το άρθρωμα πυρήνα της συμβατότητας Linux.

Το system call vector του Linux περιέχει, μεταξύ άλλων, μια λίστα με τα δεδομένα του sysent[] των οποίων οι διευθύνσεις βρίσκονται μέσα στο άρθρωμα του πυρήνα.

Όταν γίνεται μια κλήση συστήματος από μια εφαρμογή Linux, ο κώδικας (trap code) τροποποιεί τον δείκτη της μέσω της δομής που έχει εγγραφεί στο proc, και αλλάζει την διεύθυνση ώστε να δείχνει στο σημείο εισόδου της συνάρτησης του Linux, και όχι του FreeBSD.

Επίσης, το σύστημα συμβατότητας με Linux μπορεί και προσαρμόζει δυναμικά τις τοποθεσίες αναζήτησης. Ουσιαστικά αυτό κάνει και η επιλογή union κατά την προσάρτηση ενός συστήματος αρχείων (*δεν* εννοούμε εδώ το σύστημα αρχείων unionfs!). Αρχικά, γίνεται απόπειρα να βρεθεί το αρχείο στον κατάλογο /compat/linux/original-path, *και μόνο* αν αυτό αποτύχει, θα γίνει αναζήτηση στον κατάλογο /original-path. Με τον τρόπο αυτό σιγουρεύουμε ότι τα εκτελέσιμα που χρειάζονται άλλα εκτελέσιμα θα τρέξουν (για παράδειγμα, το σύνολο εργαλείων του Linux μπορεί να εκτελεστεί μέσω της υποστήριξης του Linux ABI). Επίσης σημαίνει ότι τα εκτελέσιμα του Linux μπορούν να φορτώσουν και να εκτελέσουν αρχεία του FreeBSD αν δεν μπορούν να εντοπίσουν τα αντίστοιχα αρχεία στο Linux. Μπορείτε επίσης να τοποθετήσετε μια εντολή uname(1) μέσα στο /compat/linux προκειμένου τα αρχεία του Linux να μη μπορούν να αναγνωρίσουν ότι δεν χρησιμοποιούνται πραγματικά σε Linux.

Ουσιαστικά, υπάρχει ένας πυρήνας Linux μέσα στον πυρήνα του FreeBSD. Οι διάφορες λειτουργίες οι οποίες υλοποιούν όλες τις υπηρεσίες που παρέχονται από τον πυρήνα είναι ίδιες τόσο στον πίνακα κλήσεων συστήματος του FreeBSD όσο και στον αντίστοιχο του Linux: λειτουργίες του συστήματος αρχείων, εικονική μνήμη, διαχείριση σημάτων, System V IPC κλπ. Η μόνη διαφορά είναι ότι το εκτελέσιμα του FreeBSD κάνουν χρήση των συναρτήσεων *glue* του FreeBSD, ενώ τα εκτελέσιμα του Linux, κάνουν χρήση των συναρτήσεων *glue* του Linux (πολλά από τα παλιά λειτουργικά είχαν τις δικές τους συναρτήσεις *glue*: οι διευθύνσεις των συναρτήσεων βρίσκονταν στο στατικό πίνακα sysent[], αντί να διευκρινίζονται μέσω ενός δυναμικού δείκτη στη δομή proc της διεργασίας που πραγματοποιεί την κλήση).

Ποιο είναι όμως το εγγενές FreeBSD ABI; Δεν έχει και πολύ σημασία. Η μόνη βασική διαφορά είναι (κάτι το οποίο μπορεί εύκολα να αλλάξει σε μελλοντικές εκδόσεις, και πολύ πιθανόν να αλλάξει) ότι οι συναρτήσεις *glue* του FreeBSD είναι στατικά συνδεδεμένες στο πυρήνα, ενώ οι αντίστοιχες του Linux μπορούν είτε να είναι συνδεδεμένες στατικά, είτε να είναι προσβάσιμες μέσω ενός αρθρώματος πυρήνα.

Είναι αυτό όμως πραγματική εξομοίωση; Όχι. Είναι μια υλοποίηση του ABI, όχι εξομοίωση. Δεν

υπάρχει καμία εξομοίωση (ή προσομοίωση, για να προλάβουμε την επόμενη σας ερώτηση).

Τότε γιατί μερικές φορές μιλάμε για "εξομοίωση Linux"; Για να δυσκολευτεί η προώθηση του FreeBSD! Η αρχική υλοποίηση έγινε την εποχή όπου δεν υπήρχε άλλη λέξη που να μπορούσε να περιγράψει το τι ακριβώς γινόταν. Το να λέγαμε ότι το FreeBSD έτρεχε εκτελέσιμα Linux δεν θα ήταν αλήθεια, μια και χρειαζόταν να ενσωματωθεί κάποιος κώδικας στον πυρήνα, ή να φορτωθεί κάποιο άρθρωμα. Χρειαζόταν κάποια λέξη που να περιγράφει τι φορτωνόταν-έτσι προέκυψε ο "εξομοιωτής Linux".

params: path: "/books/handbook/partiii/" :leveloffset: +1

Part III: Ρύθμιση και Βελτιστοποίηση

Chapter 18. Σύνοψη

Ένα από τα σημαντικά χαρακτηριστικά του FreeBSD είναι η δυνατότητα ρύθμισης του συστήματος. Με τις σωστές ρυθμίσεις συστήματος είναι εύκολο να αποφευχθούν πολλά προβλήματα κατά τη διάρκεια μελλοντικών αναβαθμίσεων. Το κεφάλαιο αυτό θα εξηγήσει μεγάλο μέρος της διαδικασίας ρύθμισης του FreeBSD, συμπεριλαμβανομένων και κάποιων παραμέτρων που μπορούν να ρυθμιστούν για την βελτιστοποίηση της απόδοσης του συστήματος.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να δουλέψετε αποδοτικά με συστήματα αρχείων και κατατμήσεις swap.
- Τα βασικά των συστημάτων ρύθμισης και εκκίνησης rc.conf και /usr/local/etc/rc.d.
- Πως να ρυθμίσετε και να δοκιμάσετε μια κάρτα δικτύου.
- Πως να ρυθμίσετε virtual hosts στις δικτυακές σας συσκευές.
- Πως να χρησιμοποιήσετε τα διάφορα αρχεία ρυθμίσεων στον κατάλογο /etc.
- Πως να βελτιστοποιήσετε το FreeBSD χρησιμοποιώντας μεταβλητές `sysctl`.
- Πως να βελτιστοποιήσετε την απόδοση του δίσκου και να αλλάξετε τους περιορισμούς του πυρήνα.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε βασικές έννοιες του UNIX® και του FreeBSD (Βασικές Έννοιες στο UNIX®).
- Να είστε εξοικειωμένοι με τα βασικά της ρύθμισης και της μεταγλώττισης του πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).

Chapter 19. Αρχική Ρύθμιση

19.1. Διάταξη Κατατμήσεων

19.1.1. Βασικές Κατατμήσεις

Όταν δημιουργείτε συστήματα αρχείων με το bsdlabel(8) ή το sysinstall(8), θυμηθείτε ότι οι σκληροί δίσκοι μεταφέρουν δεδομένα γρηγορότερα απο τα εξωτερικά μέροι τους στα εσωτερικά. Έτσι μικρότερα και περισσότερο προσβάσιμα συστήματα αρχείων πρέπει να είναι πλησιέστερα στο εξωτερικό του δίσκου, ενώ μεγαλύτερες κατατμήσεις όπως το /usr πρέπει να τοποθετούνται πιο κοντά στο εσωτερικό του δίσκου. Είναι καλή ιδέα να δημιουργείτε κατατμήσεις με παρόμοια σειρά με αυτήν: root, swap, /var, /usr.

Το μέγεθος του /var αντανακλά την επιδιωκούμενη χρήση του μηχανήματος. Το /var χρησιμοποιείτε για την αποθήκευση των γραμματοκιβωτίων, των αρχείων καταγραφής και του spooler του εκτυπωτή. Τα γραμματοκιβώτια και τα αρχεία καταγραφής μπορούν να μεγαλώσουν σε απροσδόκητα μεγέθη ανάλογα με τον αριθμό των χρηστών του συστήματος και το χρονικό διάστημα που κρατούνται τα αρχεία καταγραφής. Σπάνια χρειάζεται το /var/tmp να έχει πάνω από ένα gigabyte χώρο, αλλά καλό είναι να έχετε κατά νου ότι πρέπει να είναι αρκετά μεγάλο για να κρατάει τα πακέτα που θέλετε να εγκαταστήσετε.

Η κατάτμηση /usr περιέχει τα περισσότερα αρχεία που απαιτούνται για την υποστήριξη του συστήματος, τη συλλογή των ports(7) (προτείνεται) και τον πηγαίο κώδικα (προαιρετικό). Και τα δύο αυτά είναι προαιρετικά κατα την εγκατάσταση. Τουλάχιστον 2 gigabytes προτείνονται για αυτή την κατάτμηση.

Όταν επιλέγετε μέγεθος για τις κατατμήσεις, να έχετε υπόψιν σας τις απαιτήσεις σε χώρο. Μπορεί να είναι λίγο πρόβλημα το να μείνετε χωρίς χώρο σε μια κατάτμηση ενώ χρησιμοποιείτε ελάχιστα μια άλλη.

Μερικές φορές η επιλογή `Auto-defaults` του κατατμητή του sysinstall(8) μπορεί να επιλέξει πολύ μικρό μέγεθος για τις κατατμήσεις /var και /. Προσπαθείστε να επιλέξετε έξυπνα και γενναιόδωρα μεγέθη για τις κατατμήσεις σας.

19.1.2. Swap Κατάτμηση

Ένας εμπειρικός κανόνας για να επιλέξετε μέγεθος για την κατάτμηση swap είναι: πρέπει να είναι περίπου διπλή απο το μέγεθος της μνήμης (RAM) του συστήματος. Για παράδειγμα, αν το μηχάνημα έχει 128 megabytes μνήμης, η κατάτμηση swap πρέπει να είναι 256 megabytes. Συστήματα με λιγότερη μνήμη μπορούν να αποδίδουν καλύτερα με περισσότερο swap. Λιγότερο απο 256 megabytes swap δεν προτείνεται και πρέπει να εξεταστεί η επέκταση της μνήμης. Οι αλγόριθμοι VM paging του πυρήνα είναι έτσι φτιαγμένοι ώστε να αποδίδουν καλύτερα όταν η κατάτμηση swap είναι τουλάχιστον δύο φορές το μέγεθος της κεντρικής μνήμης. Αν ρυθμίσετε πολύ μικρό swap, μπορεί να έχουν μειωμένη απόδοση οι αλγόριθμοι σάρωσης σελίδων του υποσυστήματος VM και μπορεί αργότερα να δημιουργηθούν προβλήματα αν προστεθεί περισσότερη φυσική μνήμη.

Σε μεγαλύτερα συστήματα με πολλαπλούς SCSI δίσκους (ή πολλαπλούς IDE δίσκους σε

διαφορετικούς ελεγκτές), είναι προτιμότερο το swap να είναι ρυθμισμένο σε κάθε δίσκο (μέχρι τέσσερις δίσκους). Οι ξεχωριστές κατατμήσεις swap καλό είναι να έχουν περίπου το ίδιο μέγεθος. Ο πυρήνας μπορεί να χειριστεί αυθαίρετα μεγέθη swap, αλλά οι εσωτερικές δομές δεδομένων ρυθμίζονται με βάση το μέγεθος της μεγαλύτερης κατάτμησης swap. Κρατώντας την κατάτμηση swap σχεδόν στο ίδιο μέγεθος θα επιτρέψει στον πυρήνα να βελτιστοποιήσει την χρήση του swap, μοιράζοντας πιο καλά το φόρτο σε κάθε δίσκο. Δεν πειράζει να έχετε μεγάλο μέγεθος swap, ακόμα και αν δε χρησιμοποιείται αρκετά. Μπορεί να είναι ευκολότερη η ανάκαμψη απο ένα εκτός ελέγχου πρόγραμμα προτού χρειαστεί να επανεκκινήσετε το σύστημα.

19.1.3. Γιατί να φτιάξετε κατατμήσεις;

Αρκετοί χρήστες νομίζουν ότι μία μεγάλη κατάτμηση θα είναι εντάξει, αλλά υπάρχουν αρκετοί λόγοι γιατί αυτό είναι κακή ιδέα. Καταρχήν, κάθε κατάτμηση έχει διαφορετικά λειτουργικά χαρακτηριστικά, οπότε ξεχωρίζοντας τις κατατμήσεις επιτρέπουμε στο σύστημα αρχείων να εναρμονίζεται ανάλογα. Για παράδειγμα, οι root και /usr κατατμήσεις είναι κυρίως για ανάγνωση, χωρίς πολλές εγγραφές. Αντίθετα, γίνονται πολλές αναγνώσεις και εγγραφές στις /var και /var/tmp.

Κάνοντας σωστή κατάτμηση σε ένα σύστημα, ο κατακερματισμός που συμβαίνει σε μικρότερες και περισσότερο εγγράψιμες κατατμήσεις δεν θα διαρρεύσει στις κατατμήσεις που διαβάζονται πιο συχνά από ότι γράφονται. Κρατώντας τις περισσότερο εγγράψιμες κατατμήσεις πιο κοντά στην άκρη του δίσκου, θα αυξηθεί η I/O απόδοση στις κατατμήσεις όπου και χρειάζεται πιο συχνά. Τώρα ενώ η απόδοση I/O χρειάζεται στις μεγαλύτερες κατατμήσεις, αλλάζοντας αυτές πιο κοντά στην άκρη του δίσκου δεν θα οδηγήσει σε σημαντική αύξηση της απόδοσης όσο το να μετακινήσετε την /var στην άκρη. Τέλος, υπάρχει και θέμα ασφάλειας. Μία μικρή, προσεγμένη root κατάτμηση η οποία είναι διαβάζεται πιο συχνά από ότι γράφεται έχει μεγαλύτερη πιθανότητα να επιζήσει ενός άσχημου χτυπήματος.

Chapter 20. Κύρια Ρύθμιση

Η κύρια τοποθεσία των πληροφοριών για την ρύθμιση του συστήματος βρίσκεται μέσα στο /etc/rc.conf. Αυτό το αρχείο περιέχει ένα ευρύ φάσμα ρυθμίσεων, κυρίως χρησιμοποιούμενες στην εκκίνηση του συστήματος για την ρύθμιση του συστήματος. Το όνομα του απευθείας συνεπάγεται αυτό; είναι ρυθμίσεις για τα αρχεία rc*.

Ένας διαχειριστής πρέπει να δημιουργήσει εγγραφές μέσα στο αρχείο rc.conf ώστε να αντικαταστήσει τις προεπιλεγμένες ρυθμίσεις απο το αρχείο /etc/defaults/rc.conf. Το αρχείο προεπιλογών δεν πρέπει να αντιγραφεί αυτολεξεί στο /etc - αυτό περιέχει προεπιλεγμένες τιμές, όχι παραδείγματα. Όλες οι αλλαγές που αφορούν το σύστημα πρέπει να γίνουν στο αρχείο rc.conf αποκλειστικά.

Ένας αριθμός στρατηγικών μπορεί να εφαρμοστεί σε ένα σύνολο εφαρμογών για να ξεχωρίσουμε ρυθμίσεις του ευρύ συνόλου απο τις ρυθμίσεις επικεντρωμένες για ένα σύστημα για να κρατήσουμε τον φόρτο διαχείρισης χαμηλά. Η προτεινόμενη προσέγγιση είναι να τοποθετούμε τις ρυθμίσεις ευρύ συνόλου σε ένα διαφορετικό αρχείο, όπως το /etc/rc.conf.site, και τότε να συμπεριλάβουμε το αρχείο αυτό στο /etc/rc.conf, το οποίο θα περιέχει πληροφορίες επικεντρωμένες για ένα σύστημα.

Μιάς και το rc.conf διαβάζεται απο το sh(1) είναι εύκολο να το επιτύχουμε αυτό. Για παράδειγμα:

- rc.conf:

```
. /etc/rc.conf.site
hostname="node15.example.com"
network_interfaces="fxp0 lo0"
ifconfig_fxp0="inet 10.1.1.1"
```

- rc.conf.site:

```
defaultrouter="10.1.1.254"
saver="daemon"
blanktime="100"
```

Το αρχείο rc.conf.site μπορεί έπειτα να διανεμηθεί σε κάθε σύστημα χρησιμοποιώντας το `rsync` ή κάποιο παρόμοιο πρόγραμμα, ενώ το αρχείο rc.conf παραμένει μοναδικό.

Αναβαθμίζοντας το σύστημα χρησιμοποιώντας sysinstall(8) ή `make world` δεν θα αντικαταστήσει το αρχείο rc.conf, έτσι οι ρυθμίσεις δεν θα χαθούν.

Chapter 21. Ρύθμιση Εφαρμογών

Τυπικά, οι εγκατεστημένες εφαρμογές έχουν τα δικά τους αρχεία ρυθμίσεων, με το δικό τους τρόπο σύνταξης, κτλπ. Είναι σημαντικό αυτά τα αρχεία να κρατούνται ξεχωριστά απο το βασικό σύστημα, έτσι ώστε να είναι εύκολα εντοπίσιμα και διαχειρίσιμα απο τα εργαλεία διαχείρισης πακέτων.

Τυπικά, αυτά τα αρχεία είναι εγκατεστημένα στο /usr/local/etc. Σε αυτή την περίπτωση όταν μία εφαρμογή έχει μεγάλο αριθμό αρχείων ρυθμίσεων, ένας υποκατάλογος δημιουργείται για να τα αποθηκεύσει.

Κανονικά, όταν ένα port ή ένα package εγκαθιστάτε, παραδείγματα αρχείων ρυθμίσεων εγκαθιστάνται επίσης. Αυτά είναι συνήθως αναγνωρίσιμα απο την .default κατάληξη τους. Αν δεν υπάρχουν αρχεία ρυθμίσεων για την εφαρμογή, τότε θα δημιουργηθούν κάνοντας αντιγραφή τα .default αρχεία.

Για παράδειγμα, έχετε υπόψη σας τα περιεχόμενα του καταλόγου /usr/local/etc/apache:

```
-rw-r--r--  1 root  wheel   2184 May 20  1998 access.conf
-rw-r--r--  1 root  wheel   2184 May 20  1998 access.conf.default
-rw-r--r--  1 root  wheel   9555 May 20  1998 httpd.conf
-rw-r--r--  1 root  wheel   9555 May 20  1998 httpd.conf.default
-rw-r--r--  1 root  wheel  12205 May 20  1998 magic
-rw-r--r--  1 root  wheel  12205 May 20  1998 magic.default
-rw-r--r--  1 root  wheel   2700 May 20  1998 mime.types
-rw-r--r--  1 root  wheel   2700 May 20  1998 mime.types.default
-rw-r--r--  1 root  wheel   7980 May 20  1998 srm.conf
-rw-r--r--  1 root  wheel   7933 May 20  1998 srm.conf.default
```

Τα μεγέθοι των αρχείων δείχνουν ότι μόνο το αρχείο srm.conf έχει αλλάξει. Μία μετέπειτα αναβάθμιση του port της εφαρμογής Apache δεν θα αντικαταστήσει το αλλαγμένο αρχείο.

Chapter 22. Εκκινώντας Υπηρεσίες

Πολλοί χρήστες επιλέγουν να εγκαταστήσουν λογισμικό απο τρίτους κατασκευαστές στο FreeBSD απο την συλλογή των Ports. Σε πολλές απο αυτές τις περιπτώσεις μπορεί να είναι απαραίτητο να ρυθμίσουν το λογισμικό με τέτοιο τρόπο ώστε να μπορεί να επιτραπεί η εκκίνηση του κατα την εκκίνηση του συστήματος. Υπηρεσίες, όπως το mail/postfix ή το www/apache13 είναι μόνο δύο απο τα πολλά πακέτα λογισμικού που μπορεί να χρειάζονται να εκκινηθούν κατά την εκκίνηση του συστήματος. Το μέρος αυτό θα εξηγήσει τις διαθέσιμες διαδικασίες για την εκκίνηση λογισμικού προερχόμενο απο τρίτους κατασκευαστές.

Στο FreeBSD, οι περισσότερες περιεχόμενες υπηρεσίες, όπως το cron(8), είναι εκκινήσιμες μέσα από τα σενάρια εκκίνησης του συστήματος. Τα σενάρια αυτά μπορεί να διαφέρουν ανάλογα το FreeBSD ή την έκδοση του κατασκευαστή; ωστόσο, η πιο σημαντική πτυχή που πρέπει να εξεταστεί είναι ότι οι ρυθμίσεις εκκίνησης τους μπορούν να χειριστούν μέσα απο ένα απλό σενάριο εκκίνησης.

Πριν την έλευση του rc.d, οι εφαρμογές μπορούσαν να τοποθετήσουν ένα απλό σενάριο εκκίνησης μέσα στον κατάλογο /usr/local/etc/rc.d ο οποίος μπορούσε να διαβαστεί απο τα σενάρια εκκίνησης του συστήματος. Αυτά τα σενάρια μπορούσαν να εκτελεστούν κατα τα μετέπειτα στάδια εκκίνησης του συστήματος.

Ενώ πολλοί ιδιώτες ξόδευαν χρόνο προσπαθώντας να συνχωνεύσουν το παλιό στυλ ρυθμίσεων με το νέο στυλ, παραμένει γεγονός ότι μερικά προγράμματα ακόμα απαιτούν ένα σενάριο να τοποθετηθεί μέσα στον προαναφερθέντα κατάλογο. Οι λεπτές διαφορές ανάμεσα στα σενάρια εξαρτώνται από το αν ή όχι ο rc.d χρησιμοποιείτε. Προγενέστερα του FreeBSD 5.1 το παλιό στυλ ρυθμίσεων χρησιμοποιούνταν και σχεδόν σε όλες τις περιπτώσεις ένα νέου στυλ σενάριο θα είναι συμβατό.

Ενώ κάθε σενάριο πρέπει να τηρεί ορισμένες ελάχιστες απαιτήσεις, τις περισσότερες φορές αυτές οι απαιτήσεις είναι ανεξάρτητες της έκδοσης του FreeBSD. Κάθε σενάριο πρέπει να έχει μια .sh επέκταση προσαρτημένη στο τέλος του και κάθε σενάριο πρέπει να είναι εκτελέσιμο απο το σύστημα. Το δεύτερο μπορεί να επιτευχθεί χρησιμοποιώντας την `chmod` εντολή και ρυθμίζοντας την άδεια `755`. Εκεί πρέπει να υπάρχει, τουλάχιστον, μια επιλογή `start` και μία επιλογή `stop` για την εφαρμογή.

Το πιο απλό σενάριο εκκίνησης πιθανότατα να μοιάζει με το παρακάτω:

```
#!/bin/sh
echo -n ' utility'

case "$1" in
start)
        /usr/local/bin/utility
        ;;
stop)
        kill -9 `cat /var/run/utility.pid`
        ;;
*)
        echo "Usage: `basename $0` {start|stop}" >&2
        exit 64
        ;;
```

```
esac

exit 0
```

Το σενάριο αυτό παρέχει μια `stop` και μια `start` επιλογή για την εφαρμογή όπου στο παράδειγμα εδώ αναφέρεται σαν `utility`.

Μπορεί να εκκινηθεί χειρωνακτικά κάνοντας:

```
# /usr/local/etc/rc.d/utility.sh start
```

Παρόλο που δεν απαιτούν όλες οι εφαρμογές να προστεθεί μία εγγραφή στο rc.conf, σχεδόν καθημερινά και ένα νέο port θα τροποποιήτε για να δέχεται αυτή την ρύθμιση. Ελέγξετε την τελική έξοδο της εγκατάστασης για περισσότερες πληροφορίες πάνω στην συγκεκριμένη εφαρμογή. Μερικές εφαρμογές απο τρίτους κατασκευαστές παρέχουν σενάρια εκκίνησης τα οποία επιτρέπουν στην εφαρμογή να χρησιμοποιηθεί με το rc.d, παρόλα αυτα, αυτό θα συζητηθεί στο επόμενο μέρος.

22.1. Εκτεταμένη Ρύθμιση Εφαρμογών

Πλέον το FreeBSD περιέχει το rc.d, η ρύθμιση της εκκίνησης των εφαρμογών έχει γίνει ευκολότερη, και πιο πλούσια σε χαρακτηρικά. Χρησιμοποιώντας λέξεις κλειδία μέσα στον κατάλογο rc.d, οι εφαρμογές μπορούν πλέον να εκκινούν έπειτα απο συγκεκριμένες υπηρεσίες για παράδειγμα την DNS, μπορεί να επιτραπεί η εισαγωγή επιπλέον παραμέτρων μέσα απο το rc.conf στην θέση των ήδη υπάρχοντον παραμέτρων απο τα σενάρια εκκινήσης, κτλπ. Ένα βασικό σενάριο μπορεί να μοιάζει με το ακόλουθο:

```
#!/bin/sh
#
# PROVIDE: utility
# REQUIRE: DAEMON
# KEYWORD: shutdown

. /etc/rc.subr

name=utility
rcvar=utility_enable

command="/usr/local/sbin/utility"

load_rc_config $name

#
# DO NOT CHANGE THESE DEFAULT VALUES HERE
# SET THEM IN THE /etc/rc.conf FILE
#
utility_enable=${utility_enable-"NO"}
pidfile=${utility_pidfile-"/var/run/utility.pid"}
```

```
run_rc_command "$1"
```

Το σενάριο αυτό θα εξασφαλίσει ότι το πρόγραμμα utility θα εκκινηθεί μετά απο την `daemon` υπηρεσία. Θα εξασφαλίσει επιπλέον έναν τρόπο για την ρύθμιση και τον εντοπισμό του PID, ή του αρχείου του ID της διεργασίας.

Η εφαρμογή μπορεί πλέον να έχει την παρακάτω γραμμή τοποθετημένη στο /etc/rc.conf:

```
utility_enable="YES"
```

Ο νέος αυτός τρόπος επιτρέπει επιπλέον τον ευκολότερο χειρισμό των παραμέτρων της γραμμής εντολών, σε συνδυασμό με τις προυπάρχουσες λειτουργίες παρεχόμενες απο το /etc/rc.subr, τη συμβατότητα με το βοηθητικό πρόγραμμα rcorder(8) και επιπλέον την ευκολότερη ρύθμιση μέσω του rc.conf αρχείου.

22.2. Χρησιμοποιώντας Υπηρεσίες Για Την Εκκίνηση Υπηρεσιών

Άλλες υπηρεσίες, όπως ο δαίμονας του εξυπηρετή POP3, IMAP, κτλπ. μπορούν να εκκινηθούν χρησιμοποιώντας το inetd(8). Αυτό απαιτεί την εγκατάσταση του βοηθητικού προγράμματος υπηρεσιών απο την Ports συλλογή και μια γραμμή ρυθμίσεων προσαρτημένη στο αρχείο /etc/inetd.conf, ή αποχαρακτηρίζοντας μια απο τις ήδη υπάρχουσες γραμμές ρυθμίσεων. Δουλεύοντας με το inetd και τις ρυθμίσεις του περιγράφεται αναλυτικά στο μέρος inetd.

Σε πολλές περιπτώσεις, είναι εύλογο να χρησιμοποιείτε ο δαίμονας cron(8) για την εκκίνηση των υπηρεσιών του συστήματος. Η προσέγγιση αυτή έχει έναν αριθμό πλεονεκτημάτων γιατί το `cron` τρέχει τις διεργασίες σαν ιδιοκτήτης του crontab αρχείου. Αυτό επιτρέπει στους κανονικούς χρήστες να εκκινούν και να διαχειρίζονται μερικές εφαρμογές.

Το βοηθητικό πρόγραμμα `cron` παρέχει ένα μοναδικό χαρακτηριστικό, το `@reboot`, το οποίο μπορεί να χρησιμοποιηθεί στην θέση του χρονικού ορισμού. Αυτό θα κάνει την εργασία να τρέξει όταν το cron(8) εκκινηθεί, συνήθως κατά την εκκίνηση του συστήματος.

Chapter 23. Ρυθμίζοντας Το Πρόγραμμα `cron`

Ένα απο τα πιο χρήσιμα βοηθητικά προγράμματα στο FreeBSD είναι το cron(8). Το πρόγραμμα `cron` τρέχει στο παρασκήνιο και συνεχώς ελέγχει το αρχείο /etc/crontab. Το `cron` ελέγχει επίσης τον κατάλογο /var/cron/tabs, αναζητώντας καινούργια αρχεία crontab. Τα αρχεία crontab έχουν αποθηκευμένες πληροφορίες για συγκεκριμένες διαδικασίες τις οποίες το `cron` πρέπει να εκτελέσει σε συγκεκριμένο χρόνο.

Το `cron` χρησιμοποιεί δύο διαφορετικούς τύπους αρχείων ρυθμίσεων, το crontab του συστήματος και το crontab των χρηστών. Η μόνη διαφορά ανάμεσα στους δύο αυτούς τύπους είναι το έκτο πεδίο. Στο crontab του συστήματος, το έκτο πεδίο είναι το όνομα του χρήστη με του οποίου θα εκτελεστεί η εντολή. Αυτό δίνει την δυνατότητα στο crontab του συστήματος να εκτελεί εντολές σαν οποιοδήποτε χρήστης. Στο crontab των χρηστών, το έκτο πεδίο είναι η εντολή που πρέπει να εκτελεστεί, και όλες οι εντολές εκτελούνται στο όνομα του χρήστη που δημιούργησε το crontab; αυτό είναι ένα σημαντικό χαρακτηριστικό ασφαλείας.

Τα crontabs των χρηστών επιτρέπουν σε μεμονωμένους χρήστες να προγραμματίσουν εργασίες χωρίς την ανάγκη `root` δικαιωμάτον. Οι εντολές μέσα στο crontab ενός χρήστη τρέχουν με τα δικαιώματα του χρήστη του οποίου ανήκει το crontab.

Ο χρήστης `root` μπορεί να έχει ένα crontab χρήστη ακριβώς όπως κάθε χρήστης. Αυτό είναι διαφορετικό απο το /etc/crontab (το crontab του συστήματος). Λόγο του crontab του συστήματος, δεν υπάρχει συνήθως καμία ανάγκη για την δημιουργία ενός ξεχωριστού crontab για τον χρήστη `root`.

Ας ρίξουμε μια ματία στο αρχείο /etc/crontab (το crontab του συστήματος):

```
# /etc/crontab - root's crontab for FreeBSD
#
# $FreeBSD: src/etc/crontab,v 1.32 2002/11/22 16:13:39 tom Exp $
#①
#
SHELL=/bin/sh
PATH=/etc:/bin:/sbin:/usr/bin:/usr/sbin ②
HOME=/var/log
#
#
#minute hour    mday    month   wday    who command ③
#
#
*/5 *   *   *   *   root    /usr/libexec/atrun ④
```

① Όπως στα περισσότερα αρχεία ρυθμίσεων στο FreeBSD, ο χαρακτήρας `#` παριστάνει ένα σχόλιο. Ένα σχόλιο μπορεί να τοποθετηθεί μέσα στο αρχείο σαν υπενθύμιση για το τι πραγματοποιεί και γιατί μία ενέργεια. Τα σχόλια δεν μπορούν να είναι στην ίδια γραμμή με μία εντολή γιατί αλλιώς θα ερμηνευτούν σαν κομμάτι της εντολής; πρέπει να είναι σε μία νέα γραμμή. Οι κενές γραμμές αγνοούνται.

② Καταρχήν, πρέπει να καθοριστεί το περιβάλλον. Ο χαρακτήρας ίσον (=) χρησιμοποιείτε για να καθορίσει τις ρυθμίσεις του περιβάλλοντος, όπως σε αυτό το παράδειγμα που χρησιμοποιούνται οι μεταβλητές SHELL, PATH, και HOME. Αν η γραμμή του κέλυφους παραμεληθεί, το cron θα χρησιμοποιήσει την προεπιλεγμένη, οι οποία είναι η sh. Αν η μεταβλητή PATH παραμεληθεί, δεν θα χρησιμοποιηθεί προεπιλεγμένη και η τοποθεσίες των αρχείων θα πρέπει να καθοριστούν με ακρίβεια. Αν η HOME παραμεληθεί, το cron θα χρησιμοποιήσει τον κεντρικό κατάλογο των εκάστοτε χρηστών.

③ Η γραμμή αυτή καθορίζει συνολικά επτά πεδία. Τα πεδία αυτά είναι τα minute, hour, mday, month, wday, who, και command. Αυτά είναι απο μόνα τους επεξηγηματικά. Το πεδίο minute είναι ο χρόνος σε λεπτά τον οποίον η εντολή θα εκτελεστεί. Το πεδίο hour είναι παρόμοιο με το πεδίο minute, απλά είναι σε ώρες. Το πεδίο mday καθορίζει την ημέρα του μήνα. Το πεδίο month είναι παρόμοιο με το πεδίο hour και το πεδίο minute, υποδεικνύοντας τον μήνα. Το πεδίο wday καθορίζει την ημέρα της εβδομάδας. Όλα αυτά τα πεδία πρέπει να έχουν αριθμητικές τιμές, και να ακολουθούν το είκοσι-τετράωρο ρολόι. Το πεδίο who είναι ιδιαίτερο, και υπάρχει μόνο μέσα στο αρχείο /etc/crontab. Το πεδίο αυτό καθορίζει σαν ποιός χρήστης θα τρέξει την εντολή. Όταν ένας χρήστης εγκαθιστά το crontab αρχείο του, δεν θα έχει το πεδίο αυτό διαθέσιμο. Τέλος, θα ακολουθήσει η επιλογή command. Αυτό είναι το τελευταίο πεδίο, έτσι και λογικά υποδεικνύει την εντολή που θα εκτελεστεί.

④ Η τελευταία αυτή γραμμή θα καθορίσει τα μεγέθοι που συζητήθηκαν παραπάνω. Προσέξτε εδώ ότι έχουμε έναν ορισμό */5, ακολουθούμενο απο αρκετούς χαρακτήρες *. Οι χαρακτήρες * σημαίνουν "πρώτο-τελευταίο", και μπορούν να ερμηνευθούν σαν *κάθε* φορά. Έτσι, κρίνοντας απο αυτή την γραμμή, είναι προφανές ότι η εντολή atrun επικαλείται απο τον χρήστη root κάθε πέντε λεπτά ανεξάρτητα απο την ημέρα και τον μήνα. Για περισσότερες πληροφορίες σχετικά με την εντολή atrun, κοιτάξτε την σελίδα βοηθείας atrun(8).Οι εντολές μπορούν να έχουν απεριόριστο αριθμό παραμέτρων, ωστόσο, οι εντολές με εκτεταμένο αριθμό γραμμών πρέπει να διασπαστούν με τον χαρακτήρα συνέχειας αντίθετης καθέτου "\".

Αυτές είναι οι βασικές ρυθμίσεις για κάθε αρχείο crontab, ωστόσο υπάρχει και κάτι διαφορετικό. Το πεδίο έξι, όπου και καθορίζουμε το όνομα χρήστη, υπάρχει μόνο στο αρχείο του συστήματος /etc/crontab. Το πεδίο αυτό πρέπει να παραλειφθεί για κάθε crontab αρχείο χρήστη.

23.1. Εγκαθιστώντας Ένα Crontab

Δεν θα πρέπει να χρησιμοποιήσετε την διαδικασία που περιγράφεται εδώ για την διόρθωση/εγκατάσταση του crontab του συστήματος. Απλά χρησιμοποιήστε τον αγαπημένο σας κειμενογράφο: το cron θα εντοπίσει ότι το αρχείο έχει τροποποιηθεί και θα αρχίσει άμεσα να χρησιμοποιεί την ανανεωμένη έκδοση του. Δείτε αυτή την εγγραφή του FAQ για περισσότερες πληροφορίες.

Για να εγκαταστήσετε ένα νέο crontab χρήστη, πρώτα χρησιμοποιήστε τον αγαπημένο σας κειμενογράφο για να δημιουργήσετε ένα αρχείο με το απαιτούμενο τύπο, και τότε χρησιμοποιήστε το crontab. Η πιο κοινή χρήση του είναι:

```
% crontab crontab-file
```

Στο παράδειγμα αυτό, το αρχείο crontab-file είναι το όνομα του αρχείου crontab που είχε

δημιουργηθεί προηγουμένως.

Υπάρχει επίσης μία επιλογή για να απαριθμήσετε τα εγκατεστημένα αρχεία crontab: απλά εισάγετε την επιλογή `-l` στην εντολή `crontab` και ελέγξτε το αποτέλεσμα.

Για τους χρήστες που θέλουν να αρχίσουν το crontab αρχείο τους απο την αρχή, χωρίς την χρήση προτύπου, μπορούν να χρησιμοποιήσουν την εντολή `crontab -e`. Αυτή η εντολή θα ξεκινήσει τον κειμενογράφο με ένα κενό αρχείο. Όταν το αρχείο αποθηκευθεί, θα εγκατασταθεί αυτόματα απο την εντολή `crontab`.

Αν αργότερα θέλετε να διαγράψετε το crontab αρχείο χρήστη τελείως, χρησιμοποιήστε την εντολή `crontab` μαζί με την επιλογή `-r`.

Chapter 24. Χρησιμοποιώντας Το Σύστημα rc Στο FreeBSD

Το 2002 το FreeBSD ενσωμάτωσε το σύστημα rc.d του NetBSD για την εκκίνηση του συστήματος. Οι χρήστες θα πρέπει να έχουν αντιληφθεί τα αρχεία που βρίσκονται στον κατάλογο /etc/rc.d. Πολλά απο αυτά τα αρχεία είναι για τις βασικές υπηρεσίες και μπορούν να ελεγθούν με τις επιλογές `start`, `stop`, και `restart`. Για παράδειγμα, το sshd(8) μπορεί να ελεγθεί χρησιμοποιώντας την εξής εντολή:

```
# /etc/rc.d/sshd restart
```

Η διαδικασία αυτή είναι παρόμοια και για τις υπόλοιπες υπηρεσίες. Φυσικά, οι υπηρεσίες αυτές είναι συνήθως αυτόματα εκκινήσιμες κατα την εκκίνηση του συστήματος όπως και καθορίζεται στο rc.conf(5). Για παράδειγμα, ενεργοποιώντας τον δαίμονα Network Address Translation στην εκκίνηση είναι τόσο απλό όσο κάνοντας προσθήκη της ακόλουθης γραμμής στο /etc/rc.conf:

```
natd_enable="YES"
```

Αν η επιλογή `natd_enable="NO"` είναι ήδη παρούσα, τότε απλά αλλάζετε την επιλογή `NO` σε `YES`. Τα σενάρια rc θα φορτώσουν αυτόματα οποιαδήποτε εξαρτώμενη υπηρεσία κατά την διάρκεια της επόμενης εκκίνησης, όπως και περιγράφεται παρακάτω.

Μιας και το σύστημα rc.d είναι κυρίως για την εκκίνηση και τον τερματισμό υπηρεσιών κατα την εκκίνηση και τον τερματισμό του συστήματος αντίστοιχα, οι προκαθορισμένες επιλογές `start`, `stop` και `restart` θα πραγματοποιήσουν τις αντίστοιχες ενέργειες αν η κατάλληλες μεταβλητές είναι καθορισμένες στο /etc/rc.conf. Για παράδειγμα η παραπάνω εντολή `sshd restart` θα δουλέψει μόνο αν η μεταβλητή `sshd_enable` έχει τεθεί σε `YES` μέσα στο /etc/rc.conf. Για να εκτελέσετε τις επιλογές `start`, `stop` ή `restart` μιας υπηρεσίας ανεξάρτητα απο τις ρυθμίσεις της στο /etc/rc.conf, η εντολή πρέπει να έχει χαρακτηριστεί με "one". Για παράδειγμα για την επανεκκίνηση του `sshd` ανεξάρτητα απο τις τρέχουσες ρυθμίσεις στο /etc/rc.conf, εκτελείτε την ακόλουθη εντολή:

```
# /etc/rc.d/sshd onerestart
```

Είναι εύκολο να ελέγξετε αν η υπηρεσία είναι ενεργοποιημένη στο /etc/rc.conf τρέχοντας το κατάλληλο σενάριο rc.d με την παράμετρο `rcvar`. Κατά συνέπεια, ένας διαχειριστής μπορεί να ελέγξει αν το `sshd` είναι όντως ενεργοποιημένο στο /etc/rc.conf εκτελώντας:

```
# /etc/rc.d/sshd rcvar
# sshd
$sshd_enable=YES
```

Η δεύτερη γραμμή (`# sshd`) είναι η έξοδος της εντολής `sshd`, και όχι η κονσολά του χρήστη `root`.

Για να ελέγξετε αν μια υπηρεσία τρέχει, η επιλογή `status` είναι διαθέσιμη. Για παράδειγμα για να επιβεβαιώστε ότι η υπηρεσία `sshd` τρέχει:

```
# /etc/rc.d/sshd status sshd is
      running as pid 433.
```

Σε πολλές περιπτώσεις είναι δυνατόν το `reload` μίας υπηρεσίας. Αυτό θα στείλει ένα σήμα στην υπηρεσία, επιβάλλοντας της να ξαναφορτώσει τα αρχεία ρυθμίσεων της. Στην πραγματικότητα αυτό σημαίνει ότι θα στείλει ένα σήμα `SIGHUP` στην υπηρεσία. Η υποστήριξη για αυτό το χαρακτηριστικό δεν παρέχεται σε κάθε υπηρεσία.

Το σύστημα rc.d δεν χρησιμοποιείτε μόνο για τις υπηρεσίες δικτύου, αλλά επίσης συμβάλει και κατα την εκκίνηση του συστήματος. Για παράδειγμα, σκεφτείτε το αρχείο bgfsck. Όταν ένα σενάριο εκτελείτε, θα εκτυπώνει το ακόλουθο μήνυμα:

```
Starting background file system checks in 60 seconds.
```

Επομένος το αρχείο αυτό χρησιμοποιείτε στο παρασκήνιο για τον έλεγχο του συστήματος αρχείων, ο οποίος και συμβαίνει κατα στην εκκίνηση του συστήματος.

Πολλές υπηρεσίες εξαρτώνται από άλλες υπηρεσίες για να τα καταφέρουν να λειτουργήσουν σωστά. Για παράδειγμα, η υπηρεσία NIS και άλλες βασισμένες στο RPC υπηρεσίες θα αποτύχουν να εκκινηθούν αν η υπηρεσία `rpcbind` (portmapper) δεν έχει ήδη εκκινηθεί. Για να λύθει το πρόβλημα αυτό, υπάρχουν πληροφορίες για τις εξαρτήσεις και άλλα μετα-δεδομένα μέσα στα σχόλια στην αρχή κάθε σεναρίου. Το πρόγραμμα rcorder(8) χρησιμοποιείτε για την ανάλυση των σχολίων αυτών κατά την εκκίνηση του συστήματος για να καθορίστει με ποιά σειρά θα πρέπει να εκκινηθούν οι υπηρεσίες ώστε να εκπληρωθούν οι εξαρτήσεις. Οι επόμενες προτάσεις μπορούν να περιληφθούν μέσα σε κάθε αρχείο εκκίνησης:

- `PROVIDE`: Καθόριζει την υπηρεσία που παρέχει το αρχείο αυτό.
- `REQUIRE`: Απαριθμεί τις υπηρεσίες που απαιτούνται για την την υπηρεσία αυτή. Το αρχείο αυτό θα εκτελεστεί *μετά* απο την καθορισμένη υπηρεσία.
- `BEFORE`: Απαριθμεί τις υπηρεσίες οι οποίες εξαρτώνται απο την υπηρεσία αυτή. Το αρχείο αυτό θα εκτελεστεί *πρίν* τις καθορισμένες υπηρεσίες.

Χρησιμοποιώντας την μέθοδο αυτή, οι διαχειριστές μπορούν εύκολα να ελέγξουν τις υπηρεσίες του συστήματος χωρίς τα δυσνόητα "runlevels" όπως σε μερικά άλλα λειτουργικά συστήματα UNIX®.

Επιπλέον πληροφορίες για το σύστημα rc.d μπορούν να βρεθούν στις σελίδες βοηθείας rc(8) και rc.subr(8). Αν ενδιαφέρεστε για την εγγραφή δικών σας σεναρίων rc.d ή για την βελτίωση των ήδη υπάρχοντων, θα βρείτε τον σύνδεσμο αυτόν αρκετά χρήσιμο.

Chapter 25. Ρυθμίζοντας Τις Κάρτες Δικτύου

Την σήμερον εποχή δεν μπορούμε να σκεφτούμε έναν υπολογιστή χωρίς να σκεφτούμε και μία σύνδεση δικτύου. Προσθέτοντας και ρυθμίζοντας μια κάρτα δικτύου είναι μία συνηθισμένη εργασία για έναν οποιοδήποτε διαχειριστή του FreeBSD.

25.1. Εντοπίζοντας Τον Σωστό Οδηγό

Πριν αρχίσετε, θα πρέπει να γνωρίζετε το μοντέλο της κάρτας που έχετε, ποιό chip χρησιμοποιεί, και αν είναι PCI ή ISA κάρτα. Το FreeBSD υποστηρίζει ένα μεγάλο εύρος καρτών PCI και ISA. Ελέγξτε την Λίστα Συμβατότητας Υλικού για την έκδοση σας για να δείτε αν η κάρτα σας υποστηρίζεται.

Εφόσον είστε πλέον σίγουρος ότι η κάρτα σας υποστηρίζεται, θα χρειαστεί να καθορίσετε τον κατάλληλο οδηγό για την κάρτα σας. Το αρχείο /usr/src/sys/conf/NOTES και το αρχείο /usr/src/sys/arch/conf/NOTES θα σας δώσουν μια λίστα με κάρτες δικτύου και μερικές πληροφορίες για τα υποστηριζόμενα chipsets και τις υποστηριζόμενες κάρτες. Αν έχετε αμφιβολίες για το ποιός οδηγός είναι ο σωστός, διαβάστε την σελίδα βοηθείας του οδηγού. Η σελίδα βοηθείας θα σας δώσει περισσότερες πληροφορίες σχετικά με το υποστηριζόμενο υλικό και ακόμα και για τα πιθανά προβλήματα που μπορεί να προκύψουν.

Αν έχετε μια συνηθισμένη κάρτα, κατα πάσα πιθανότητα δεν θα χρειαστεί να ψάξετε πολύ για τον οδηγό. Οι οδηγοί για τις συνηθισμένες κάρτες δικτύου υπάρχουν στον πυρήνα GENERIC, έτσι ώστε και θα εμφανιστεί κατα την διάρκεια της εκκίνησης, για παράδειγμα:

```
dc0: <82c169 PNIC 10/100BaseTX> port 0xa000-0xa0ff mem 0xd3800000-0xd38
000ff irq 15 at device 11.0 on pci0
dc0: Ethernet address: 00:a0:cc:da:da:da
miibus0: <MII bus> on dc0
ukphy0: <Generic IEEE 802.3u media interface> on miibus0
ukphy0:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
dc1: <82c169 PNIC 10/100BaseTX> port 0x9800-0x98ff mem 0xd3000000-0xd30
000ff irq 11 at device 12.0 on pci0
dc1: Ethernet address: 00:a0:cc:da:da:db
miibus1: <MII bus> on dc1
ukphy1: <Generic IEEE 802.3u media interface> on miibus1
ukphy1:  10baseT, 10baseT-FDX, 100baseTX, 100baseTX-FDX, auto
```

Στο παράδειγμα αυτό, βλέπουμε ότι δύο κάρτες που χρησιμοποιούν τον οδηγό dc(4) έχουν εντοπιστεί στο σύστημα.

Αν ο οδηγός της NIC σας δεν είναι παρόν στον GENERIC, θα πρέπει να φορτώσετε τον κατάλληλο οδηγό για να χρησιμοποιήσετε την NIC σας. Αυτό μπορεί να επιτευχθεί με έναν απο τους δύο αυτούς τρόπους:

- Ο ποιό εύκολο τρόπος είναι απλά να φορτώσετε ένα άρθρωμα του πυρήνα για την κάρτα δικτύου σας με το kldload(8), ή αυτόματα κατα την εκκίνηση προσθέτοντας την κατάλληλη γραμμή στο αρχείο /boot/loader.conf. Δεν είναι όλοι οι οδηγοί NIC διαθέσιμοι σαν αρθρώματα, χαρακτηριστικά παραδείγματα είναι τα αρθρώματα για συσκευές ISA.

- Εναλλακτικά, μπορείτε να μεταγλώττισετε στατικά την υποστήριξη για την κάρτα σας στον πυρήνα. Ελέγξετε το αρχείο /usr/src/sys/conf/NOTES, το /usr/src/sys/arch/conf/NOTES και την σελίδα βοηθείας του οδηγού για να μάθετε τι πρέπει να προσθέσετε στο αρχείο ρυθμίσεων του πυρήνα. Για περισσότερες πληροφορίες για το πως να μεταγλωττίσετε τον πυρήνα, παρακαλώ διαβάστε το Ρυθμίζοντας τον Πυρήνα του FreeBSD. Αν η κάρτα σας εντοπιστεί κατα την εκκίνηση απο τον πυρήνα (GENERIC) δεν χρειάζετε να μεταγλώττισετε έναν νέο πυρήνα.

25.1.1. Χρησιμοποιώντας Οδηγούς Windows® Με Το NDIS

Δυστυχώς, υπάρχουν ακόμα πολλοί κατασκευαστές που δεν παρέχουν τεχνικές προδιαγραφές για τους οδηγούς τους στην κοινότητα του ανοικτού λογισμικού γιατί αντιμετωπίζουν τέτοιες πληροφορίες σαν μυστικά του εμπορίου. Συνεπώς, οι υπεύθυνοι για την ανάπτυξη του FreeBSD και άλλων λειτουργικών συστημάτων μένουν με δύο επιλογές: να αναπτύξουν οδηγούς με την μακρά και επίπονη διαδικασία της αντίστροφης μηχανικής ή να χρησιμοποιήσουν ήδη υπάρχοντες οδηγούς σε δυαδική μορφή διαθέσιμους για την πλατφόρμα Microsoft® Windows®. Οι περισσότεροι υπεύθυνοι για την ανάπτυξη, μεταξύ τους και αυτοί που εμπλέκονται με το FreeBSD, έχουν επιλέξει την δεύτερη προσέγγιση.

Χάρη την προσφορά του Bill Paul (wpaul), μιάς και απο το FreeBSD 5.3-RELEASE υπάρχει "γηγενής" υποστήριξη για το Network Driver Interface Specification (NDIS). Το έργο FreeBSD NDISulator (διαφορετικά γνωστό σας Project Evil) παίρνει έναν οδηγό Windows® σε δυαδική μορφή και στην ουσία τον εξαπατά ώστε να νομίζει ότι τρέχει σε Windows®. Λόγο του ότι ο οδηγός ndis(4) χρησιμοποιεί μία Windows® δυαδική μορφή, μπορεί να χρησιμοποιηθεί μόνο σε i386™ και amd64 συστήματα.

Ο οδηγός ndis(4) είναι σχεδιασμένος ώστε να υποστηρίζει κυρίως συσκευές PCI, CardBus και PCMCIA, οι συσκευές USB δεν υποστηρίζονται ακόμα.

Για να χρησιμοποιήσετε τον NDISulator, θα χρειαστείτε τρία πράγματα:

1. Τον πηγαίο κώδικα του πυρήνα
2. Την Windows® XP δυαδική μορφή του οδηγού (.SYS επέκταση)
3. Το Windows® XP αρχείο ρυθμίσεων του οδηγού (.INF επέκταση)

Εντοπίστε τα αρχεία αυτά για την κάρτα σας. Γενικά, αυτά μπορούν να βρεθούν στα παρεχόμενα CDs ή στους ιστότοπους των κατασκευαστών. Στα ακόλουθα παραδείγματα, θα χρησιμοποιήσουμε τα αρχεία W32DRIVER.SYS και W32DRIVER.INF.

Δεν μπορείτε να χρησιμοποιήσετε οδηγούς Windows®/i386 σε συστήματα FreeBSD/amd64, θα πρέπει να βρείτε οδηγούς Windows®/amd64 για να δουλέψουν σωστά.

Το επόμενο βήμα είναι να μεταγλωττίσετε τον δυαδικό οδηγό μέσα σε ένα φορτώσιμο άρθρωμα του πυρήνα. Για να το επιτύχετε αυτό, θα πρέπει σαν `root`, να χρησιμοποιήσετε το ndisgen(8):

```
# ndisgen /path/to/W32DRIVER.INF /path/to/W32DRIVER.SYS
```

Το βοηθητικό πρόγραμμα ndisgen(8) είναι διαδραστικό και θα σας ενημερώσει για οποιαδήποτε επιπλέον πληροφορία μπορεί να χρειαστεί; θα παράγει ένα άρθρωμα του πυρήνα στον τρέχωντα κατάλογο και μπορεί να φορτωθεί ως εξής:

```
# kldload ./W32DRIVER.ko
```

Επιπλέον του παραχθέντος αρθρώματος, θα πρέπει να φορτώσετε τα αρθρώματα ndis.ko και if_ndis.ko. Αυτό θα πρέπει να γίνει αυτόματα όταν φορτώνετε οποιαδήποτε εξαρτάται απο το ndis(4). Αν θέλετε να το κάνετε χειρωνακτικά, θα πρέπει να χρησιμοποιήσετε τις ακόλουθες εντολές:

```
# kldload ndis
# kldload if_ndis
```

Η πρώτη εντολή φορτώνει τον οδηγό NDIS miniport wrapper, ενώ η δεύτερη φορτώνει την πραγματική κάρτα δικτύου.

Τώρα, ελέγξτε το dmesg(8) για να δείτε αν υπάρχουν σφάλματα κατα την φόρτωση. Αν όλα πήγαν καλά, θα πρέπει να δείτε μια παρόμοια έξοδο με την επόμενη:

```
ndis0: <Wireless-G PCI Adapter> mem 0xf4100000-0xf4101fff irq 3 at device 8.0 on pci1
ndis0: NDIS API version: 5.0
ndis0: Ethernet address: 0a:b1:2c:d3:4e:f5
ndis0: 11b rates: 1Mbps 2Mbps 5.5Mbps 11Mbps
ndis0: 11g rates: 6Mbps 9Mbps 12Mbps 18Mbps 36Mbps 48Mbps 54Mbps
```

Απο εδώ και πέρα μπορείτε να χειριστείτε την συσκευή ndis0 σαν μια οποιαδήποτε κάρτα δικτύου (π.χ., dc0).

Μπορείτε να ρυθμίσετε το σύστημα να φορτώνει τα NDIS αρθρώματα κατα την εκκίνηση με τον ίδιο τρόπο με τα όπως με οποιαδήποτε άλλα αρθρώματα. Πρώτα, αντιγράψτε το παραχθείσα άρθρωμα, W32DRIVER.ko, στον κατάλογο /boot/modules. Τότε, προσθέστε την ακόλουθη γραμμή στο /boot/loader.conf:

```
W32DRIVER_load="YES"
```

25.2. Ρυθμίζοντας Την Κάρτα Δικτύου

Μόλις ο κατάλληλος οδηγός φορτωθεί για την κάρτα δικτύου, χρειάζεται να ρυθμιστεί. Όπως πολλά άλλα πράγματα, η κάρτα δικτύου είχε ρυθμιστεί κατα την στιγμή της εγκατάστασης με το sysinstall.

Για να εμφανίσετε τις κάρτες δικτύου που έχετε στο σύστημα σας, πληκτρολογήστε την ακόλουθη εντολή:

```
% ifconfig
```

```
dc0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 192.168.1.3 netmask 0xffffff00 broadcast 192.168.1.255
        ether 00:a0:cc:da:da:da
        media: Ethernet autoselect (100baseTX <full-duplex>)
        status: active
dc1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
        ether 00:a0:cc:da:da:db
        media: Ethernet 10baseT/UTP
        status: no carrier
lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1 netmask 0xff000000
tun0: flags=8010<POINTOPOINT,MULTICAST> mtu 1500
```

Παλαιότερες εκδόσεις του FreeBSD μπορεί να χρειάζονται την παράμετρο `-a` ακολουθούμενη στην ifconfig(8), για περισσότερες λεπτομέρειες σχετικά με την σωστή σύνταξη του ifconfig(8), παρακαλώ ανατρέξτε στην σελίδα βοηθείας. Σημειώστε επίσης ότι οι εγγραφές που αφορούν το IPv6 (`inet6` κτλπ.) έχουν παραμεληθεί σε αυτό το παράδειγμα.

Σε αυτό το παράδειγμα, οι ακόλουθες συσκευές έχουν εμφανιστεί:

- dc0: Η πρώτη Ethernet κάρτα δικτύου
- dc1: Η δεύτερη Ethernet κάρτα δικτύου
- lp0: Η παράλληλη πόρτα
- lo0: Η συσκευή loopback
- tun0: Η συσκευή tunnel χρησιμοποιούμενη απο το πρόγραμμα ppp

Το FreeBSD χρησιμοποιεί τα ονόματα των οδηγών με την σειρά κατα την οποία εντοπίστηκαν οι αντίστοιχες κάρτες κατα την εκκίνηση. Για παράδειγμα η συσκευή sis2 θα είναι η τρίτη κάρτα δικτύου που χρησιμοποιεί τον οδηγό sis(4).

Στο παράδειγμα αυτό, η συσκευή dc0 είναι πάνω και τρέχει. Οι λέξεις κλειδία είναι:

1. `UP` σημαίνει ότι η κάρτα είναι ρυθμισμένη και έτοιμη.
2. Η κάρτα έχει μία Internet διεύθυνση (`inet`) ρυθμισμένη (σε αυτή την περίπτωση `192.168.1.3`).
3. Έχει μία έγκυρη μάσκα υποδικτύου (`netmask`; `0xffffff00` είναι το ίδιο με το `255.255.255.0`).
4. Έχει μία έγκυρη broadcast διεύθυνση (σε αυτή την περίπτωση, `192.168.1.255`).
5. Η διεύθυνση MAC της κάρτας (`ether`) είναι `00:a0:cc:da:da:da`
6. Η επιλογή του φυσικού μέσου είναι σε κατάσταση autoselection (`media: Ethernet autoselect (100baseTX <full-duplex>)`). Παρατηρούμε ότι η dc1 έχει ρυθμιστεί να τρέχει σαν `10baseT/UTP` μέσο. Για περισσότερες πληροφορίες για τους τύπους των μέσων ενός οδηγού, παρακαλώ ανατρέξτε στην σελίδα βοηθείας.
7. Η κατάσταση της σύνδεσης (`status`) είναι `active`, δηλ. έχει εντοπιστεί σήμα μεταφοράς. Στην dc1,

παρατηρούμε `status: no carrier`. Αυτό είναι λογικό αφού το καλώδιο Ethernet δεν έχει συνδεθεί με την κάρτα.

Αν το ifconfig(8) εμφανίζει κάτι παρόμοιο με αυτό:

```
dc0: flags=8843<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
            ether 00:a0:cc:da:da:da
```

σημαίνει ότι η κάρτα δεν έχει ρυθμιστεί.

Για να ρυθμίσετε την κάρτα σας, θα χρειαστείτε προνόμια `root`. Η ρύθμιση της κάρτας δικτύου μπορεί να γίνει απο την γραμμή εντολών με το ifconfig(8) αλλά θα πρέπει να το επαναλάβετε σε κάθε επανεκκίνηση του συστήματος. Το αρχείο /etc/rc.conf είναι εκεί όπου πρέπει να προσθέσετε τις ρύθμισεις της κάρτας δικτύου.

Ανοίξτε το αρχείο /etc/rc.conf με τον αγαπημένο σας κειμενογράφο. Θα χρειαστεί να προσθέσετε μία γραμμή για κάθε κάρτα δικτύου που υπάρχει στο σύστημα σας, για παράδειγμα στην περίπτωση μας, θα πρέπει να προσθέσετε τι εξής γραμμές:

```
ifconfig_dc0="inet 192.168.1.3 netmask 255.255.255.0"
ifconfig_dc1="inet 10.0.0.1 netmask 255.255.255.0 media 10baseT/UTP"
```

Θα πρέπει να αντικαταστήσετε το dc0, dc1, και ούτω κάθε εξής, με τις σωστές συσκευές των καρτών σας, και τις σωστές διευθύνσεις. Θα πρέπει να διαβάσετε την σελίδα βοηθείας του οδηγού και του ifconfig(8) για περισσότερες λεπτομέριες σχετικά με τις επιτρεπόμενες παραμέτρους και επίσης την σελίδα βοηθείας του rc.conf(5) για περισσότερες λεπτομέριες σχετικά με την σύνταξη του /etc/rc.conf.

Αν ρυθμίσατε το δίκτυο σας κατα την εγκατάσταση, μερικές γραμμές σχετικές με την/τις κάρτα/κάρτες δικτύου θα υπάρχουν ήδη. Ελέγξτε διπλά το /etc/rc.conf προτού προσθέστε επιπλέον γραμμές.

Θα πρέπει επίσης να διορθώσετε το αρχείο /etc/hosts ώστε να προσθέσετε τα ονόματα και τις IP διεύθυνσεις απο τα διάφορα μηχανήματα στο LAN σας, αν δεν είναι ήδη ρυθμισμένα. Για περισσότερες πληροφορίες ανατρέξτε στην σελίδα βοηθείας του hosts(5) και του /usr/shared/examples/etc/hosts.

25.3. Δοκιμές Και Επίλυση Προβλημάτων

Μόλις κάνετε τις βασικές αλλαγές στο /etc/rc.conf, θα πρέπει να επανεκκινήσετε το σύστημα σας. Αυτό θα επιτρέψει σε πιθανές αλλαγές στις κάρτες να εφαρμοστούν, και να επιβεβαιώσετε ότι το σύστημα επανεκκινεί χωρίς κανένα λάθος στις ρυθμίσεις.

Μόλις το σύστημα επανεκκινηθεί, θα πρέπει να δοκιμάσετε τις κάρτες δικτύου.

25.3.1. Δοκιμάζοντας Μια Ethernet Κάρτα

Για να επιβεβαιώσετε ότι η Ethernet κάρτα λειτουργεί σωστά, θα πρέπει να κάνετε δύο πράγματα. Πρώτα, κάντε ping την κάρτα την ίδια, και μετά κάντε ping ένα άλλο μηχάνημα στο LAN.

Πρώτα δοκιμάστε στην τοπική κάρτα:

```
% ping -c5 192.168.1.3
PING 192.168.1.3 (192.168.1.3): 56 data bytes
64 bytes from 192.168.1.3: icmp_seq=0 ttl=64 time=0.082 ms
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.074 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.076 ms
64 bytes from 192.168.1.3: icmp_seq=3 ttl=64 time=0.108 ms
64 bytes from 192.168.1.3: icmp_seq=4 ttl=64 time=0.076 ms

--- 192.168.1.3 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.074/0.083/0.108/0.013 ms
```

Τώρα δοκιμάστε σε ένα άλλο μηχάνημα στο LAN:

```
% ping -c5 192.168.1.2
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=0.726 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.766 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.700 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.747 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.704 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.700/0.729/0.766/0.025 ms
```

Μπορείτε να χρησιμοποιήσετε και το όνομα το μηχανήματος αντί της διεύθυνσης `192.168.1.2` αν έχετε ρυθμίσει το αρχείο /etc/hosts.

25.3.2. Επίλυση Προβλημάτων

Η επίλυση προβλημάτων υλικού και λογισμικού είναι πάντοτε επίπονη, ένας πόνος ο οποιός μπορεί να ανακουφιστεί ελέγχοντας μερικά απλά πράγματα πρώτα. Είναι το καλώδιο του δικτύου συνδεδεμένο; Έχετε ρυθμίσει σωστά τις υπηρεσίες δικτύου; Έχετε ρυθμίσει σωστά το πύρινο τείχος; Έχει πράγματι το FreeBSD υποστήριξη για αυτή την κάρτα δικτύου; Πρέπει πάντα να ελέγχετε τις σημειώσεις του υλικού πριν στείλε μία αναφορά για ένα πρόβλημα. Αναβαθμίστε την έκδοση του FreeBSD στην τελευταία ΣΤΑΘΕΡΗ έκδοση. Ελέγξτε τα αρχεία των λιστών μηνυμάτων, ή ψάξτε στο Internet.

Αν η κάρτα δουλεύει, αλλά με χαμηλή απόδοση, θα άξιζε να διαβάσετε την σελίδα βοηθείας tuning(7). Μπορείτε επίσης να ελέγξετε οι αν λανθασμένες ρυθμίσεις του δικτύου προκαλούν τις

αργές συνδέσεις.

Μερικοί χρήστες αντιμετωπίζουν ένα ή δύο μηνύματα `device timeout`, τα οποία είναι φυσιολογικά για μερικές κάρτες. Αν συνεχιστούν, ή γίνουν ενοχλητικά, θα πρέπει να ελέγξετε μήπως και κάποιες συσκευές παρεμποδίζουν η μία την άλλη. Ελέγξτε διπλά τις συνδέσεις των καλωδίων. Ίσως θα πρέπει να αποκτήσετε μία άλλη κάρτα.

Μερικές φορές, οι χρήστες παρατηρούν μερικά μηνύματα λάθους `watchdog timeout`. Το πρώτο πράγμα που πρέπει να κάνετε είναι να ελέγξετε το καλώδιο του δικτύου. Αρκέτες κάρτες χρειάζονται μία θέση PCI που να υποστηρίζει Bus Mastering. Σε μερικές παλιές μητρικές κάρτες. μόνο μία θέση PCI το υποστήριζε (συνήθως η θέση 0). Ελέγξτε την κάρτα δικτύου και την τεκμηρίωση της μητρικής κάρτας για να διαπιστώσετε αν εκεί είναι το πρόβλημα.

Το μήνυμα `No route to host` εμφανίζεται αν το σύστημα αδυνατεί να δρομολογήσει τα πακέτα στον προορισμό τους. Αυτό συμβαίνει αν δεν έχει καθοριστεί προεπιλεγμένη διεύθυνση δρομολόγησης, ή αν ένα καλώδιο έχει ξεσυνδεθεί. Ελέγξτε την έξοδο τις εντολής `netstat -rn` και σιγουρευτείτε ότι η διεύθυνση δρομολόγησης είναι έγκυρη. Αν δεν έχει καθοριστεί, διαβάστε το Προχωρημένα Θέματα Δικτύωσης για περισσότερες πληροφορίες.

Το μήνυμα λάθους `ping: sendto: Permission denied` συμβαίνει κυρίως λόγο κάποιας λάθος ρύθμισης στο πύρινο τείχος. Αν το `ipfw` είναι ενεργοποιημένο στον πυρήνα αλλά δεν έχουν καθοριστεί κανόνες, τότε η προεπιλεγμένη πολιτική είναι η απαγόρευση όλης της κίνησης, ακόμα και των αιτημάτων ping! Διαβάστε το Firewalls για περισσότερες πληροφορίες.

Μερικές φορές η απόδοση της κάρτας μπορεί να είναι φτωχή, ή κάτω του μέσου όρου. Σε αυτές τις περιπτώσεις το καλύτερο είναι να ρυθμίσετε την κατάσταση του μέσου απο `autoselect` στην κατάλληλη κατάσταση. Ενώ συνήθως αυτό φαίνετε να δουλεύει στα περισσότερα υλικά, μπορεί να μην λύσει το πρόβλημα στον καθέναν. Και πάλι, ελέγξτε όλες τις ρυθμίσεις του δικτύου, και ξαναδιαβάστε πάλι την σελίδα βοηθείας tuning(7).

Chapter 26. Εικονικά Hosts

Μία αρκετά συνηθισμένη χρήση του FreeBSD είναι η εικονική φιλοξενία ιστοχώρων, όπου και ένας εξυπηρετητής εμφανίζεται στο δίκτυο σαν περισσότερο απο ένας. Αυτό επιτυγχάνεται αναθέτοντας πολλαπλές δικτυακές διευθύνσεις σε μία και μόνο συσκευή.

Μία κάρτα δικτύου έχει μία "πραγματική" διεύθυνση, και απεριόριστο αριθμό "εικονικών" διευθύνσεων. Οι εικονικές αυτές διεύθυνσεις προσθέτονται με την μορφή εγγραφών στο αρχείο /etc/rc.conf.

Μία εγγραφή εικονικής διεύθυνσης για την κάρτα δικτύου fxp0 μοιάζει ως εξής:

```
ifconfig_fxp0_alias0="inet xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx"
```

Σημειώστε ότι οι εγγραφές αυτές πρέπει να ξεκινούν με `alias0` και να συνεχίζουν πρός τα πάνω σε σειρά, (για παράδειγμα, `_alias1`, `_alias2`, και ούτω κάθε εξής). Η διαδικασία ρύθμισης θα σταματήσει στον πρώτο αριθμό που λείπει.

Ο υπολογισμός της μάσκας δικτύου είναι σημαντικός, αλλά ευτυχώς και εύκολος. Για κάθε κάρτα, πρέπει να υπάρχει μία διεύθυνση η οποία αντιπροσωπεύει σωστά την μάσκα του δικτύου. Οποιαδήποτε άλλη διεύθυνση που συμπίπτει στο ίδιο δίκτυο πρέπει να έχει μάσκα δικτύου `1`s (εκφρασμένη είτε σαν `255.255.255.255` είτε σαν `0xffffffff`).

Για παράδειγμα, εξετάστε την περίπτωση όπου η κάρτα δικτύου fxp0 είναι συνδεδεμένη σε δύο δίκτυα, το δίκτυο `10.1.1.0` με μάσκα δικτύου `255.255.255.0` και το δίκτυο `202.0.75.16` με μάσκα δικτύου `255.255.255.240`. Θέλουμε το σύστημα να πάρει τις διευθύνσεις από `10.1.1.1` μέχρι `10.1.1.5` και τις `202.0.75.17` μέχρι `202.0.75.20`. Όπως σημειώθηκε παραπάνω, μόνο η πρώτες διευθύνσεις (στην περίπτωση αυτή, η `10.0.1.1` και η `202.0.75.17`) πρέπει να έχουν πραγματικές μάσκες δικτύου. Όλες οι υπόλοιπες, από (`10.1.1.2` μέχρι `10.1.1.5` και `202.0.75.18` μέχρι `202.0.75.20`) πρέπει να ρυθμιστούν με μάσκα δικτύου `255.255.255.255`.

Η ακόλουθες εγγραφές στο αρχείο /etc/rc.conf θα ρυθμίσουν την κάρτα όπως πρέπει για το παράδειγμα:

```
ifconfig_fxp0="inet 10.1.1.1 netmask 255.255.255.0"
ifconfig_fxp0_alias0="inet 10.1.1.2 netmask 255.255.255.255"
ifconfig_fxp0_alias1="inet 10.1.1.3 netmask 255.255.255.255"
ifconfig_fxp0_alias2="inet 10.1.1.4 netmask 255.255.255.255"
ifconfig_fxp0_alias3="inet 10.1.1.5 netmask 255.255.255.255"
ifconfig_fxp0_alias4="inet 202.0.75.17 netmask 255.255.255.240"
ifconfig_fxp0_alias5="inet 202.0.75.18 netmask 255.255.255.255"
ifconfig_fxp0_alias6="inet 202.0.75.19 netmask 255.255.255.255"
ifconfig_fxp0_alias7="inet 202.0.75.20 netmask 255.255.255.255"
```

Chapter 27. Αρχεία Ρυθμίσεων

27.1. Ο κατάλογος /etc

Τα αρχεία ρυθμίσεων αποθηκεύονται σε καταλόγους. Μερικοί απο αυτούς είναι:

/etc	Γενικές ρυθμίσεις του συστήματος, data here is system-specific.
/etc/defaults	Default versions of system configuration files.
/etc/mail	Extra sendmail(8) configuration, other MTA configuration files.
/etc/ppp	Configuration for both user- and kernel-ppp programs.
/etc/namedb	Default location for named(8) data. Normally named.conf and zone files are stored here.
/usr/local/etc	Configuration files for installed applications. May contain per-application subdirectories.
/usr/local/etc/rc.d	Start/stop scripts for installed applications.
/var/db	Automatically generated system-specific database files, such as the package database, the locate database, and so on

27.2. Hostnames

27.2.1. /etc/resolv.conf

/etc/resolv.conf dictates how FreeBSD's resolver accesses the Internet Domain Name System (DNS).

The most common entries to resolv.conf are:

`nameserver`	The IP address of a name server the resolver should query. The servers are queried in the order listed with a maximum of three.
`search`	Search list for hostname lookup. This is normally determined by the domain of the local hostname.
`domain`	The local domain name.

A typical resolv.conf:

```
search example.com
nameserver 147.11.1.11
```

```
nameserver 147.11.100.30
```

Only one of the `search` and `domain` options should be used.

If you are using DHCP, dhclient(8) usually rewrites resolv.conf with information received from the DHCP server.

27.2.2. /etc/hosts

/etc/hosts is a simple text database reminiscent of the old Internet. It works in conjunction with DNS and NIS providing name to IP address mappings. Local computers connected via a LAN can be placed in here for simplistic naming purposes instead of setting up a named(8) server. Additionally, /etc/hosts can be used to provide a local record of Internet names, reducing the need to query externally for commonly accessed names.

```
# $FreeBSD$
#
# Host Database
# This file should contain the addresses and aliases
# for local hosts that share this file.
# In the presence of the domain name service or NIS, this file may
# not be consulted at all; see /etc/nsswitch.conf for the resolution order.
#
#
::1                     localhost localhost.my.domain myname.my.domain
127.0.0.1               localhost localhost.my.domain myname.my.domain

#
# Imaginary network.
#10.0.0.2               myname.my.domain myname
#10.0.0.3               myfriend.my.domain myfriend
#
# According to RFC 1918, you can use the following IP networks for
# private nets which will never be connected to the Internet:
#
#       10.0.0.0        -   10.255.255.255
#       172.16.0.0      -   172.31.255.255
#       192.168.0.0     -   192.168.255.255
#
# In case you want to be able to connect to the Internet, you need
# real official assigned numbers.  PLEASE PLEASE PLEASE do not try
# to invent your own network numbers but instead get one from your
# network provider (if any) or from the Internet Registry (ftp to
# rs.internic.net, directory `/templates').
#
```

/etc/hosts takes on the simple format of:

```
[Internet address] [official hostname] [alias1] [alias2] ...
```

For example:

```
10.0.0.1 myRealHostname.example.com myRealHostname foobar1 foobar2
```

Consult hosts(5) for more information.

27.3. Log File Configuration

27.3.1. syslog.conf

syslog.conf is the configuration file for the syslogd(8) program. It indicates which types of `syslog` messages are logged to particular log files.

```
# $FreeBSD$
#
#       Spaces ARE valid field separators in this file. However,
#       other *nix-like systems still insist on using tabs as field
#       separators. If you are sharing this file between systems, you
#       may want to use only tabs as field separators here.
#       Consult the syslog.conf(5) manual page.
*.err;kern.debug;auth.notice;mail.crit          /dev/console
*.notice;kern.debug;lpr.info;mail.crit;news.err /var/log/messages
security.*                                      /var/log/security
mail.info                                       /var/log/maillog
lpr.info                                        /var/log/lpd-errs
cron.*                                          /var/log/cron
*.err                                           root
*.notice;news.err                               root
*.alert                                         root
*.emerg                                         *
# uncomment this to log all writes to /dev/console to /var/log/console.log
#console.info                                   /var/log/console.log
# uncomment this to enable logging of all log messages to /var/log/all.log
#*.*                                            /var/log/all.log
# uncomment this to enable logging to a remote log host named loghost
#*.*                                            @loghost
# uncomment these if you're running inn
# news.crit                                     /var/log/news/news.crit
# news.err                                      /var/log/news/news.err
# news.notice                                   /var/log/news/news.notice
!startslip
*.*                                             /var/log/slip.log
!ppp
*.*                                             /var/log/ppp.log
```

Consult the syslog.conf(5) manual page for more information.

27.3.2. newsyslog.conf

newsyslog.conf is the configuration file for newsyslog(8), a program that is normally scheduled to run by cron(8). newsyslog(8) determines when log files require archiving or rearranging. logfile is moved to logfile.0, logfile.0 is moved to logfile.1, and so on. Alternatively, the log files may be archived in gzip(1) format causing them to be named: logfile.0.gz, logfile.1.gz, and so on.

newsyslog.conf indicates which log files are to be managed, how many are to be kept, and when they are to be touched. Log files can be rearranged and/or archived when they have either reached a certain size, or at a certain periodic time/date.

```
# configuration file for newsyslog
# $FreeBSD$
#
# filename          [owner:group]    mode count size when [ZB] [/pid_file] [sig_num]
/var/log/cron                           600  3     100  *     Z
/var/log/amd.log                        644  7     100  *     Z
/var/log/kerberos.log                   644  7     100  *     Z
/var/log/lpd-errs                       644  7     100  *     Z
/var/log/maillog                        644  7     *    @T00  Z
/var/log/sendmail.st                    644  10    *    168   B
/var/log/messages                       644  5     100  *     Z
/var/log/all.log                        600  7     *    @T00  Z
/var/log/slip.log                       600  3     100  *     Z
/var/log/ppp.log                        600  3     100  *     Z
/var/log/security                       600  10    100  *     Z
/var/log/wtmp                           644  3     *    @01T05 B
/var/log/daily.log                      640  7     *    @T00  Z
/var/log/weekly.log                     640  5     1    $W6D0 Z
/var/log/monthly.log                    640  12    *    $M1D0 Z
/var/log/console.log                    640  5     100  *     Z
```

Consult the newsyslog(8) manual page for more information.

27.4. sysctl.conf

sysctl.conf looks much like rc.conf. Values are set in a `variable=value` form. The specified values are set after the system goes into multi-user mode. Not all variables are settable in this mode.

To turn off logging of fatal signal exits and prevent users from seeing processes started from other users, the following tunables can be set in sysctl.conf:

```
# Do not log fatal signal exits (e.g. sig 11)
kern.logsigexit=0

# Prevent users from seeing information about processes that
```

```
# are being run under another UID.
security.bsd.see_other_uids=0
```

Chapter 28. Tuning with sysctl

sysctl(8) is an interface that allows you to make changes to a running FreeBSD system. This includes many advanced options of the TCP/IP stack and virtual memory system that can dramatically improve performance for an experienced system administrator. Over five hundred system variables can be read and set using sysctl(8).

At its core, sysctl(8) serves two functions: to read and to modify system settings.

To view all readable variables:

```
% sysctl -a
```

To read a particular variable, for example, `kern.maxproc`:

```
% sysctl kern.maxproc
kern.maxproc: 1044
```

To set a particular variable, use the intuitive *variable=value* syntax:

```
# sysctl kern.maxfiles=5000
kern.maxfiles: 2088 -> 5000
```

Settings of sysctl variables are usually either strings, numbers, or booleans (a boolean being `1` for yes or a `0` for no).

If you want to set automatically some variables each time the machine boots, add them to the /etc/sysctl.conf file. For more information see the sysctl.conf(5) manual page and the sysctl.conf.

28.1. sysctl(8) Read-only

In some cases it may be desirable to modify read-only sysctl(8) values. While this is sometimes unavoidable, it can only be done on (re)boot.

For instance on some laptop models the cardbus(4) device will not probe memory ranges, and fail with errors which look similar to:

```
cbb0: Could not map register memory
device_probe_and_attach: cbb0 attach returned 12
```

Cases like the one above usually require the modification of some default sysctl(8) settings which are set read only. To overcome these situations a user can put sysctl(8) "OIDs" in their local /boot/loader.conf. Default settings are located in the /boot/defaults/loader.conf file.

Fixing the problem mentioned above would require a user to set

`hw.pci.allow_unsupported_io_range=1` in the aforementioned file. Now cardbus(4) will work properly.

Chapter 29. Tuning Disks

29.1. Sysctl Variables

29.1.1. vfs.vmiodirenable

The vfs.vmiodirenable sysctl variable may be set to either 0 (off) or 1 (on); it is 1 by default. This variable controls how directories are cached by the system. Most directories are small, using just a single fragment (typically 1 K) in the file system and less (typically 512 bytes) in the buffer cache. With this variable turned off (to 0), the buffer cache will only cache a fixed number of directories even if you have a huge amount of memory. When turned on (to 1), this sysctl allows the buffer cache to use the VM Page Cache to cache the directories, making all the memory available for caching directories. However, the minimum in-core memory used to cache a directory is the physical page size (typically 4 K) rather than 512 bytes. We recommend keeping this option on if you are running any services which manipulate large numbers of files. Such services can include web caches, large mail systems, and news systems. Keeping this option on will generally not reduce performance even with the wasted memory but you should experiment to find out.

29.1.2. vfs.write_behind

The vfs.write_behind sysctl variable defaults to 1 (on). This tells the file system to issue media writes as full clusters are collected, which typically occurs when writing large sequential files. The idea is to avoid saturating the buffer cache with dirty buffers when it would not benefit I/O performance. However, this may stall processes and under certain circumstances you may wish to turn it off.

29.1.3. vfs.hirunningspace

The vfs.hirunningspace sysctl variable determines how much outstanding write I/O may be queued to disk controllers system-wide at any given instance. The default is usually sufficient but on machines with lots of disks you may want to bump it up to four or five *megabytes*. Note that setting too high a value (exceeding the buffer cache's write threshold) can lead to extremely bad clustering performance. Do not set this value arbitrarily high! Higher write values may add latency to reads occurring at the same time.

There are various other buffer-cache and VM page cache related sysctls. We do not recommend modifying these values, the VM system does an extremely good job of automatically tuning itself.

29.1.4. vm.swap_idle_enabled

The vm.swap_idle_enabled sysctl variable is useful in large multi-user systems where you have lots of users entering and leaving the system and lots of idle processes. Such systems tend to generate a great deal of continuous pressure on free memory reserves. Turning this feature on and tweaking the swapout hysteresis (in idle seconds) via vm.swap_idle_threshold1 and vm.swap_idle_threshold2 allows you to depress the priority of memory pages associated with idle processes more quickly then the normal pageout algorithm. This gives a helping hand to the pageout daemon. Do not turn this option on unless you need it, because the tradeoff you are making is essentially pre-page

memory sooner rather than later; thus eating more swap and disk bandwidth. In a small system this option will have a determinable effect but in a large system that is already doing moderate paging this option allows the VM system to stage whole processes into and out of memory easily.

29.1.5. hw.ata.wc

FreeBSD 4.3 flirted with turning off IDE write caching. This reduced write bandwidth to IDE disks but was considered necessary due to serious data consistency issues introduced by hard drive vendors. The problem is that IDE drives lie about when a write completes. With IDE write caching turned on, IDE hard drives not only write data to disk out of order, but will sometimes delay writing some blocks indefinitely when under heavy disk loads. A crash or power failure may cause serious file system corruption. FreeBSD's default was changed to be safe. Unfortunately, the result was such a huge performance loss that we changed write caching back to on by default after the release. You should check the default on your system by observing the `hw.ata.wc` sysctl variable. If IDE write caching is turned off, you can turn it back on by setting the kernel variable back to 1. This must be done from the boot loader at boot time. Attempting to do it after the kernel boots will have no effect.

For more information, please see ata(4).

29.1.6. SCSI_DELAY (kern.cam.scsi_delay)

The `SCSI_DELAY` kernel config may be used to reduce system boot times. The defaults are fairly high and can be responsible for `15` seconds of delay in the boot process. Reducing it to `5` seconds usually works (especially with modern drives). Newer versions of FreeBSD (5.0 and higher) should use the `kern.cam.scsi_delay` boot time tunable. The tunable, and kernel config option accept values in terms of *milliseconds* and *not seconds*.

29.2. Soft Updates

The tunefs(8) program can be used to fine-tune a file system. This program has many different options, but for now we are only concerned with toggling Soft Updates on and off, which is done by:

```
# tunefs -n enable /filesystem
# tunefs -n disable /filesystem
```

A filesystem cannot be modified with tunefs(8) while it is mounted. A good time to enable Soft Updates is before any partitions have been mounted, in single-user mode.

Soft Updates drastically improves meta-data performance, mainly file creation and deletion, through the use of a memory cache. We recommend to use Soft Updates on all of your file systems. There are two downsides to Soft Updates that you should be aware of: First, Soft Updates guarantees filesystem consistency in the case of a crash but could very easily be several seconds (even a minute!) behind updating the physical disk. If your system crashes you may lose more work than otherwise. Secondly, Soft Updates delays the freeing of filesystem blocks. If you have a filesystem (such as the root filesystem) which is almost full, performing a major update, such as `make installworld`, can cause the filesystem to run out of space and the update to fail.

29.2.1. More Details about Soft Updates

There are two traditional approaches to writing a file systems meta-data back to disk. (Meta-data updates are updates to non-content data like inodes or directories.)

Historically, the default behavior was to write out meta-data updates synchronously. If a directory had been changed, the system waited until the change was actually written to disk. The file data buffers (file contents) were passed through the buffer cache and backed up to disk later on asynchronously. The advantage of this implementation is that it operates safely. If there is a failure during an update, the meta-data are always in a consistent state. A file is either created completely or not at all. If the data blocks of a file did not find their way out of the buffer cache onto the disk by the time of the crash, fsck(8) is able to recognize this and repair the filesystem by setting the file length to 0. Additionally, the implementation is clear and simple. The disadvantage is that meta-data changes are slow. An `rm -r`, for instance, touches all the files in a directory sequentially, but each directory change (deletion of a file) will be written synchronously to the disk. This includes updates to the directory itself, to the inode table, and possibly to indirect blocks allocated by the file. Similar considerations apply for unrolling large hierarchies (`tar -x`).

The second case is asynchronous meta-data updates. This is the default for Linux/ext2fs and `mount -o async` for *BSD ufs. All meta-data updates are simply being passed through the buffer cache too, that is, they will be intermixed with the updates of the file content data. The advantage of this implementation is there is no need to wait until each meta-data update has been written to disk, so all operations which cause huge amounts of meta-data updates work much faster than in the synchronous case. Also, the implementation is still clear and simple, so there is a low risk for bugs creeping into the code. The disadvantage is that there is no guarantee at all for a consistent state of the filesystem. If there is a failure during an operation that updated large amounts of meta-data (like a power failure, or someone pressing the reset button), the filesystem will be left in an unpredictable state. There is no opportunity to examine the state of the filesystem when the system comes up again; the data blocks of a file could already have been written to the disk while the updates of the inode table or the associated directory were not. It is actually impossible to implement a `fsck` which is able to clean up the resulting chaos (because the necessary information is not available on the disk). If the filesystem has been damaged beyond repair, the only choice is to use newfs(8) on it and restore it from backup.

The usual solution for this problem was to implement *dirty region logging*, which is also referred to as *journaling*, although that term is not used consistently and is occasionally applied to other forms of transaction logging as well. Meta-data updates are still written synchronously, but only into a small region of the disk. Later on they will be moved to their proper location. Because the logging area is a small, contiguous region on the disk, there are no long distances for the disk heads to move, even during heavy operations, so these operations are quicker than synchronous updates. Additionally the complexity of the implementation is fairly limited, so the risk of bugs being present is low. A disadvantage is that all meta-data are written twice (once into the logging region and once to the proper location) so for normal work, a performance "pessimization" might result. On the other hand, in case of a crash, all pending meta-data operations can be quickly either rolled-back or completed from the logging area after the system comes up again, resulting in a fast filesystem startup.

Kirk McKusick, the developer of Berkeley FFS, solved this problem with Soft Updates: all pending meta-data updates are kept in memory and written out to disk in a sorted sequence ("ordered meta-

data updates"). This has the effect that, in case of heavy meta-data operations, later updates to an item "catch" the earlier ones if the earlier ones are still in memory and have not already been written to disk. So all operations on, say, a directory are generally performed in memory before the update is written to disk (the data blocks are sorted according to their position so that they will not be on the disk ahead of their meta-data). If the system crashes, this causes an implicit "log rewind": all operations which did not find their way to the disk appear as if they had never happened. A consistent filesystem state is maintained that appears to be the one of 30 to 60 seconds earlier. The algorithm used guarantees that all resources in use are marked as such in their appropriate bitmaps: blocks and inodes. After a crash, the only resource allocation error that occurs is that resources are marked as "used" which are actually "free". fsck(8) recognizes this situation, and frees the resources that are no longer used. It is safe to ignore the dirty state of the filesystem after a crash by forcibly mounting it with `mount -f`. In order to free resources that may be unused, fsck(8) needs to be run at a later time. This is the idea behind the *background fsck*: at system startup time, only a *snapshot* of the filesystem is recorded. The `fsck` can be run later on. All file systems can then be mounted "dirty", so the system startup proceeds in multiuser mode. Then, background `fsck`s will be scheduled for all file systems where this is required, to free resources that may be unused. (File systems that do not use Soft Updates still need the usual foreground `fsck` though.)

The advantage is that meta-data operations are nearly as fast as asynchronous updates (i.e. faster than with *logging*, which has to write the meta-data twice). The disadvantages are the complexity of the code (implying a higher risk for bugs in an area that is highly sensitive regarding loss of user data), and a higher memory consumption. Additionally there are some idiosyncrasies one has to get used to. After a crash, the state of the filesystem appears to be somewhat "older". In situations where the standard synchronous approach would have caused some zero-length files to remain after the `fsck`, these files do not exist at all with a Soft Updates filesystem because neither the meta-data nor the file contents have ever been written to disk. Disk space is not released until the updates have been written to disk, which may take place some time after running `rm`. This may cause problems when installing large amounts of data on a filesystem that does not have enough free space to hold all the files twice.

Chapter 30. Tuning Kernel Limits

30.1. File/Process Limits

30.1.1. kern.maxfiles

kern.maxfiles can be raised or lowered based upon your system requirements. This variable indicates the maximum number of file descriptors on your system. When the file descriptor table is full, file: table is full will show up repeatedly in the system message buffer, which can be viewed with the dmesg command.

Each open file, socket, or fifo uses one file descriptor. A large-scale production server may easily require many thousands of file descriptors, depending on the kind and number of services running concurrently.

In older FreeBSD releases, the default value of kern.maxfiles is derived from the maxusers option in your kernel configuration file. kern.maxfiles grows proportionally to the value of maxusers. When compiling a custom kernel, it is a good idea to set this kernel configuration option according to the uses of your system. From this number, the kernel is given most of its pre-defined limits. Even though a production machine may not actually have 256 users connected at once, the resources needed may be similar to a high-scale web server.

As of FreeBSD 4.5, kern.maxusers is automatically sized at boot based on the amount of memory available in the system, and may be determined at run-time by inspecting the value of the read-only kern.maxusers sysctl. Some sites will require larger or smaller values of kern.maxusers and may set it as a loader tunable; values of 64, 128, and 256 are not uncommon. We do not recommend going above 256 unless you need a huge number of file descriptors; many of the tunable values set to their defaults by kern.maxusers may be individually overridden at boot-time or run-time in /boot/loader.conf (see the loader.conf(5) man page or the /boot/defaults/loader.conf file for some hints) or as described elsewhere in this document. Systems older than FreeBSD 4.4 must set this value via the kernel config(8) option maxusers instead.

In older releases, the system will auto-tune maxusers for you if you explicitly set it to 0. When setting this option, you will want to set maxusers to at least 4, especially if you are using the X Window System or compiling software. The reason is that the most important table set by maxusers is the maximum number of processes, which is set to 20 + 16 * maxusers, so if you set maxusers to 1, then you can only have 36 simultaneous processes, including the 18 or so that the system starts up at boot time and the 15 or so you will probably create when you start the X Window System. Even a simple task like reading a manual page will start up nine processes to filter, decompress, and view it. Setting maxusers to 64 will allow you to have up to 1044 simultaneous processes, which should be enough for nearly all uses. If, however, you see the dreaded error when trying to start another program, or are running a server with a large number of simultaneous users (like ftp.FreeBSD.org), you can always increase the number and rebuild.

maxusers does *not* limit the number of users which can log into your machine. It simply sets various table sizes to reasonable values considering the maximum number of users you will likely have on your system and how many processes

each of them will be running. One keyword which *does* limit the number of simultaneous remote logins and X terminal windows is `pseudo-device pty 16`. With FreeBSD 5.X, you do not have to worry about this number since the pty(4) driver is "auto-cloning"; you simply use the line `device pty` in your configuration file.

30.1.2. `kern.ipc.somaxconn`

The `kern.ipc.somaxconn` sysctl variable limits the size of the listen queue for accepting new TCP connections. The default value of `128` is typically too low for robust handling of new connections in a heavily loaded web server environment. For such environments, it is recommended to increase this value to `1024` or higher. The service daemon may itself limit the listen queue size (e.g. sendmail(8), or Apache) but will often have a directive in its configuration file to adjust the queue size. Large listen queues also do a better job of avoiding Denial of Service () attacks.

30.2. Network Limits

The `NMBCLUSTERS` kernel configuration option dictates the amount of network Mbufs available to the system. A heavily-trafficked server with a low number of Mbufs will hinder FreeBSD's ability. Each cluster represents approximately 2 K of memory, so a value of 1024 represents 2 megabytes of kernel memory reserved for network buffers. A simple calculation can be done to figure out how many are needed. If you have a web server which maxes out at 1000 simultaneous connections, and each connection eats a 16 K receive and 16 K send buffer, you need approximately 32 MB worth of network buffers to cover the web server. A good rule of thumb is to multiply by 2, so 2x32 MB / 2 KB = 64 MB / 2 kB = 32768. We recommend values between 4096 and 32768 for machines with greater amounts of memory. Under no circumstances should you specify an arbitrarily high value for this parameter as it could lead to a boot time crash. The `-m` option to netstat(1) may be used to observe network cluster use.

`kern.ipc.nmbclusters` loader tunable should be used to tune this at boot time. Only older versions of FreeBSD will require you to use the `NMBCLUSTERS` kernel config(8) option.

For busy servers that make extensive use of the sendfile(2) system call, it may be necessary to increase the number of sendfile(2) buffers via the `NSFBUFS` kernel configuration option or by setting its value in /boot/loader.conf (see loader(8) for details). A common indicator that this parameter needs to be adjusted is when processes are seen in the `sfbufa` state. The sysctl variable `kern.ipc.nsfbufs` is a read-only glimpse at the kernel configured variable. This parameter nominally scales with `kern.maxusers`, however it may be necessary to tune accordingly.

Even though a socket has been marked as non-blocking, calling sendfile(2) on the non-blocking socket may result in the sendfile(2) call blocking until enough `struct sf_buf`'s are made available.

30.2.1. `net.inet.ip.portrange.*`

The `net.inet.ip.portrange.*` sysctl variables control the port number ranges automatically bound to TCP and UDP sockets. There are three ranges: a low range, a default range, and a high range. Most network programs use the default range which is controlled by the

`net.inet.ip.portrange.first` and `net.inet.ip.portrange.last`, which default to 1024 and 5000, respectively. Bound port ranges are used for outgoing connections, and it is possible to run the system out of ports under certain circumstances. This most commonly occurs when you are running a heavily loaded web proxy. The port range is not an issue when running servers which handle mainly incoming connections, such as a normal web server, or has a limited number of outgoing connections, such as a mail relay. For situations where you may run yourself out of ports, it is recommended to increase `net.inet.ip.portrange.last` modestly. A value of `10000`, `20000` or `30000` may be reasonable. You should also consider firewall effects when changing the port range. Some firewalls may block large ranges of ports (usually low-numbered ports) and expect systems to use higher ranges of ports for outgoing connections - for this reason it is not recommended that `net.inet.ip.portrange.first` be lowered.

30.2.2. TCP Bandwidth Delay Product

The TCP Bandwidth Delay Product Limiting is similar to TCP/Vegas in NetBSD. It can be enabled by setting `net.inet.tcp.inflight.enable` sysctl variable to `1`. The system will attempt to calculate the bandwidth delay product for each connection and limit the amount of data queued to the network to just the amount required to maintain optimum throughput.

This feature is useful if you are serving data over modems, Gigabit Ethernet, or even high speed WAN links (or any other link with a high bandwidth delay product), especially if you are also using window scaling or have configured a large send window. If you enable this option, you should also be sure to set `net.inet.tcp.inflight.debug` to `0` (disable debugging), and for production use setting `net.inet.tcp.inflight.min` to at least `6144` may be beneficial. However, note that setting high minimums may effectively disable bandwidth limiting depending on the link. The limiting feature reduces the amount of data built up in intermediate route and switch packet queues as well as reduces the amount of data built up in the local host's interface queue. With fewer packets queued up, interactive connections, especially over slow modems, will also be able to operate with lower *Round Trip Times*. However, note that this feature only effects data transmission (uploading / server side). It has no effect on data reception (downloading).

Adjusting `net.inet.tcp.inflight.stab` is *not* recommended. This parameter defaults to 20, representing 2 maximal packets added to the bandwidth delay product window calculation. The additional window is required to stabilize the algorithm and improve responsiveness to changing conditions, but it can also result in higher ping times over slow links (though still much lower than you would get without the inflight algorithm). In such cases, you may wish to try reducing this parameter to 15, 10, or 5; and may also have to reduce `net.inet.tcp.inflight.min` (for example, to 3500) to get the desired effect. Reducing these parameters should be done as a last resort only.

30.3. Virtual Memory

30.3.1. `kern.maxvnodes`

A vnode is the internal representation of a file or directory. So increasing the number of vnodes available to the operating system cuts down on disk I/O. Normally this is handled by the operating system and does not need to be changed. In some cases where disk I/O is a bottleneck and the system is running out of vnodes, this setting will need to be increased. The amount of inactive and free RAM will need to be taken into account.

To see the current number of vnodes in use:

```
#  sysctl vfs.numvnodes
vfs.numvnodes: 91349
```

To see the maximum vnodes:

```
#  sysctl kern.maxvnodes
kern.maxvnodes: 100000
```

If the current vnode usage is near the maximum, increasing `kern.maxvnodes` by a value of 1,000 is probably a good idea. Keep an eye on the number of `vfs.numvnodes`. If it climbs up to the maximum again, `kern.maxvnodes` will need to be increased further. A shift in your memory usage as reported by top(1) should be visible. More memory should be active.

Chapter 31. Adding Swap Space

No matter how well you plan, sometimes a system does not run as you expect. If you find you need more swap space, it is simple enough to add. You have three ways to increase swap space: adding a new hard drive, enabling swap over NFS, and creating a swap file on an existing partition.

For information on how to encrypt swap space, what options for this task exist and why it should be done, please refer to Encrypting Swap Space of the Handbook.

31.1. Swap on a New Hard Drive

The best way to add swap, of course, is to use this as an excuse to add another hard drive. You can always use another hard drive, after all. If you can do this, go reread the discussion of swap space in Αρχική Ρύθμιση of the Handbook for some suggestions on how to best arrange your swap.

31.2. Swapping over NFS

Swapping over NFS is only recommended if you do not have a local hard disk to swap to; NFS swapping will be limited by the available network bandwidth and puts an additional burden on the NFS server.

31.3. Swapfiles

You can create a file of a specified size to use as a swap file. In our example here we will use a 64MB file called /usr/swap0. You can use any name you want, of course.

Παράδειγμα 7. Creating a Swapfile on FreeBSD

1. Be certain that your kernel configuration includes the memory disk driver (md(4)). It is default in GENERIC kernel.

```
device   md   # Memory "disks"
```

2. Create a swapfile (/usr/swap0):

```
# dd if=/dev/zero of=/usr/swap0 bs=1024k count=64
```

3. Set proper permissions on (/usr/swap0):

```
# chmod 0600 /usr/swap0
```

4. Enable the swap file in /etc/rc.conf:

```
swapfile="/usr/swap0"   # Set to name of swapfile if aux swapfile desired.
```

5. Reboot the machine or to enable the swap file immediately, type:

```
# mdconfig -a -t vnode -f /usr/swap0 -u 0 && swapon /dev/md0
```

Chapter 32. Power and Resource Management

It is important to utilize hardware resources in an efficient manner. Before ACPI was introduced, it was difficult and inflexible for operating systems to manage the power usage and thermal properties of a system. The hardware was managed by the BIOS and thus the user had less control and visibility into the power management settings. Some limited configurability was available via *Advanced Power Management (APM)*. Power and resource management is one of the key components of a modern operating system. For example, you may want an operating system to monitor system limits (and possibly alert you) in case your system temperature increased unexpectedly.

In this section of the FreeBSD Handbook, we will provide comprehensive information about ACPI. References will be provided for further reading at the end.

32.1. What Is ACPI?

Advanced Configuration and Power Interface (ACPI) is a standard written by an alliance of vendors to provide a standard interface for hardware resources and power management (hence the name). It is a key element in *Operating System-directed configuration and Power Management*, i.e.: it provides more control and flexibility to the operating system (OS). Modern systems "stretched" the limits of the current Plug and Play interfaces prior to the introduction of ACPI. ACPI is the direct successor to APM (Advanced Power Management).

32.2. Shortcomings of Advanced Power Management (APM)

The *Advanced Power Management (APM)* facility controls the power usage of a system based on its activity. The APM BIOS is supplied by the (system) vendor and it is specific to the hardware platform. An APM driver in the OS mediates access to the *APM Software Interface*, which allows management of power levels. APM should still be used for systems manufactured at or before the year 2000.

There are four major problems in APM. Firstly, power management is done by the (vendor-specific) BIOS, and the OS does not have any knowledge of it. One example of this, is when the user sets idle-time values for a hard drive in the APM BIOS, that when exceeded, it (BIOS) would spin down the hard drive, without the consent of the OS. Secondly, the APM logic is embedded in the BIOS, and it operates outside the scope of the OS. This means users can only fix problems in their APM BIOS by flashing a new one into the ROM; which is a very dangerous procedure with the potential to leave the system in an unrecoverable state if it fails. Thirdly, APM is a vendor-specific technology, which means that there is a lot of parity (duplication of efforts) and bugs found in one vendor’s BIOS, may not be solved in others. Last but not the least, the APM BIOS did not have enough room to implement a sophisticated power policy, or one that can adapt very well to the purpose of the machine.

Plug and Play BIOS (PNPBIOS) was unreliable in many situations. PNPBIOS is 16-bit technology, so

the OS has to use 16-bit emulation in order to "interface" with PNPBIOS methods.

The FreeBSD APM driver is documented in the apm(4) manual page.

32.3. Configuring ACPI

The acpi.ko driver is loaded by default at start up by the loader(8) and should *not* be compiled into the kernel. The reasoning behind this is that modules are easier to work with, say if switching to another acpi.ko without doing a kernel rebuild. This has the advantage of making testing easier. Another reason is that starting ACPI after a system has been brought up often doesn't work well. If you are experiencing problems, you can disable ACPI altogether. This driver should not and can not be unloaded because the system bus uses it for various hardware interactions. ACPI can be disabled by setting `hint.acpi.0.disabled="1"` in /boot/loader.conf or at the loader(8) prompt.

ACPI and APM cannot coexist and should be used separately. The last one to load will terminate if the driver notices the other running.

ACPI can be used to put the system into a sleep mode with acpiconf(8), the `-s` flag, and a `1-5` option. Most users will only need `1` or `3` (suspend to RAM). Option `5` will do a soft-off which is the same action as:

```
# halt -p
```

Other options are available via sysctl(8). Check out the acpi(4) and acpiconf(8) manual pages for more information.

Chapter 33. Using and Debugging FreeBSD ACPI

ACPI is a fundamentally new way of discovering devices, managing power usage, and providing standardized access to various hardware previously managed by the BIOS. Progress is being made toward ACPI working on all systems, but bugs in some motherboards' *ACPI Machine Language* (AML) bytecode, incompleteness in FreeBSD's kernel subsystems, and bugs in the Intel® ACPI-CA interpreter continue to appear.

This document is intended to help you assist the FreeBSD ACPI maintainers in identifying the root cause of problems you observe and debugging and developing a solution. Thanks for reading this and we hope we can solve your system's problems.

33.1. Submitting Debugging Information

Before submitting a problem, be sure you are running the latest BIOS version and, if available, embedded controller firmware version.

For those of you that want to submit a problem right away, please send the following information to freebsd-acpi@FreeBSD.org:

- Description of the buggy behavior, including system type and model and anything that causes the bug to appear. Also, please note as accurately as possible when the bug began occurring if it is new for you.
- The dmesg(8) output after `boot -v`, including any error messages generated by you exercising the bug.
- The dmesg(8) output from `boot -v` with ACPI disabled, if disabling it helps fix the problem.
- Output from `sysctl hw.acpi`. This is also a good way of figuring out what features your system offers.
- URL where your *ACPI Source Language* (ASL) can be found. Do *not* send the ASL directly to the list as it can be very large. Generate a copy of your ASL by running this command:

  ```
  # acpidump -dt > name-system.asl
  ```

  (Substitute your login name for *name* and manufacturer/model for *system*. Example: njl-FooCo6000.asl)

Most of the developers watch the ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT but please submit problems to ηλεκτρονική λίστα για ACPI του FreeBSD to be sure it is seen. Please be patient, all of us have full-time jobs elsewhere. If your bug is not immediately apparent, we will probably ask you to submit a PR via send-pr(1). When entering a PR, please include the same information as requested above. This will help us track the problem and resolve it. Do not send a PR without emailing ηλεκτρονική λίστα για ACPI του FreeBSD first as we use PRs as reminders of existing problems, not a reporting mechanism. It is likely that your problem has been reported by someone

before.

33.2. Background

ACPI is present in all modern computers that conform to the ia32 (x86), ia64 (Itanium), and amd64 (AMD) architectures. The full standard has many features including CPU performance management, power planes control, thermal zones, various battery systems, embedded controllers, and bus enumeration. Most systems implement less than the full standard. For instance, a desktop system usually only implements the bus enumeration parts while a laptop might have cooling and battery management support as well. Laptops also have suspend and resume, with their own associated complexity.

An ACPI-compliant system has various components. The BIOS and chipset vendors provide various fixed tables (e.g., FADT) in memory that specify things like the APIC map (used for SMP), config registers, and simple configuration values. Additionally, a table of bytecode (the *Differentiated System Description Table* DSDT) is provided that specifies a tree-like name space of devices and methods.

The ACPI driver must parse the fixed tables, implement an interpreter for the bytecode, and modify device drivers and the kernel to accept information from the ACPI subsystem. For FreeBSD, Intel® has provided an interpreter (ACPI-CA) that is shared with Linux and NetBSD. The path to the ACPI-CA source code is src/sys/contrib/dev/acpica. The glue code that allows ACPI-CA to work on FreeBSD is in src/sys/dev/acpica/Osd. Finally, drivers that implement various ACPI devices are found in src/sys/dev/acpica.

33.3. Common Problems

For ACPI to work correctly, all the parts have to work correctly. Here are some common problems, in order of frequency of appearance, and some possible workarounds or fixes.

33.3.1. Mouse Issues

In some cases, resuming from a suspend operation will cause the mouse to fail. A known work around is to add `hint.psm.0.flags="0x3000"` to the /boot/loader.conf file. If this does not work then please consider sending a bug report as described above.

33.3.2. Suspend/Resume

ACPI has three suspend to RAM (STR) states, `S1`-`S3`, and one suspend to disk state (`STD`), called `S4`. `S5` is "soft off" and is the normal state your system is in when plugged in but not powered up. `S4` can actually be implemented two separate ways. `S4`BIOS is a BIOS-assisted suspend to disk. `S4`OS is implemented entirely by the operating system.

Start by checking `sysctl hw.acpi` for the suspend-related items. Here are the results for a Thinkpad:

```
hw.acpi.supported_sleep_state: S3 S4 S5
hw.acpi.s4bios: 0
```

This means that we can use `acpiconf -s` to test `S3`, `S4`OS, and `S5`. If `s4bios` was one (`1`), we would have `S4`BIOS support instead of `S4`OS.

When testing suspend/resume, start with `S1`, if supported. This state is most likely to work since it does not require much driver support. No one has implemented `S2` but if you have it, it is similar to `S1`. The next thing to try is `S3`. This is the deepest STR state and requires a lot of driver support to properly reinitialize your hardware. If you have problems resuming, feel free to email the ηλεκτρονική λίστα για ACPI του FreeBSD list but do not expect the problem to be resolved since there are a lot of drivers/hardware that need more testing and work.

To help isolate the problem, remove as many drivers from your kernel as possible. If it works, you can narrow down which driver is the problem by loading drivers until it fails again. Typically binary drivers like nvidia.ko, X11 display drivers, and USB will have the most problems while Ethernet interfaces usually work fine. If you can properly load/unload the drivers, you can automate this by putting the appropriate commands in /etc/rc.suspend and /etc/rc.resume. There is a commented-out example for unloading and loading a driver. Try setting `hw.acpi.reset_video` to zero (`0`) if your display is messed up after resume. Try setting longer or shorter values for `hw.acpi.sleep_delay` to see if that helps.

Another thing to try is load a recent Linux distribution with ACPI support and test their suspend/resume support on the same hardware. If it works on Linux, it is likely a FreeBSD driver problem and narrowing down which driver causes the problems will help us fix the problem. Note that the ACPI maintainers do not usually maintain other drivers (e.g sound, ATA, etc.) so any work done on tracking down a driver problem should probably eventually be posted to the ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT list and mailed to the driver maintainer. If you are feeling adventurous, go ahead and start putting some debugging printf(3)s in a problematic driver to track down where in its resume function it hangs.

Finally, try disabling ACPI and enabling APM instead. If suspend/resume works with APM, you may be better off sticking with APM, especially on older hardware (pre-2000). It took vendors a while to get ACPI support correct and older hardware is more likely to have BIOS problems with ACPI.

33.3.3. System Hangs (temporary or permanent)

Most system hangs are a result of lost interrupts or an interrupt storm. Chipsets have a lot of problems based on how the BIOS configures interrupts before boot, correctness of the APIC (MADT) table, and routing of the *System Control Interrupt* (SCI).

Interrupt storms can be distinguished from lost interrupts by checking the output of `vmstat -i` and looking at the line that has `acpi0`. If the counter is increasing at more than a couple per second, you have an interrupt storm. If the system appears hung, try breaking to DDB (`CTRL` + `ALT` + `ESC` on console) and type `show interrupts`.

Your best hope when dealing with interrupt problems is to try disabling APIC support with `hint.apic.0.disabled="1"` in loader.conf.

33.3.4. Panics

Panics are relatively rare for ACPI and are the top priority to be fixed. The first step is to isolate the

steps to reproduce the panic (if possible) and get a backtrace. Follow the advice for enabling `options DDB` and setting up a serial console (see Είσοδος στον DDB Debugger Μέσω της Σειριακής Γραμμής) or setting up a dump(8) partition. You can get a backtrace in DDB with `tr`. If you have to handwrite the backtrace, be sure to at least get the lowest five (5) and top five (5) lines in the trace.

Then, try to isolate the problem by booting with ACPI disabled. If that works, you can isolate the ACPI subsystem by using various values of `debug.acpi.disable`. See the acpi(4) manual page for some examples.

33.3.5. System Powers Up After Suspend or Shutdown

First, try setting `hw.acpi.disable_on_poweroff="0"` in loader.conf(5). This keeps ACPI from disabling various events during the shutdown process. Some systems need this value set to `1` (the default) for the same reason. This usually fixes the problem of a system powering up spontaneously after a suspend or poweroff.

33.3.6. Other Problems

If you have other problems with ACPI (working with a docking station, devices not detected, etc.), please email a description to the mailing list as well; however, some of these issues may be related to unfinished parts of the ACPI subsystem so they might take a while to be implemented. Please be patient and prepared to test patches we may send you.

33.4. ASL, `acpidump`, and IASL

The most common problem is the BIOS vendors providing incorrect (or outright buggy!) bytecode. This is usually manifested by kernel console messages like this:

```
ACPI-1287: *** Error: Method execution failed [\\_SB_.PCI0.LPC0.FIGD._STA] \\
(Node 0xc3f6d160), AE_NOT_FOUND
```

Often, you can resolve these problems by updating your BIOS to the latest revision. Most console messages are harmless but if you have other problems like battery status not working, they are a good place to start looking for problems in the AML. The bytecode, known as AML, is compiled from a source language called ASL. The AML is found in the table known as the DSDT. To get a copy of your ASL, use acpidump(8). You should use both the `-t` (show contents of the fixed tables) and `-d` (disassemble AML to ASL) options. See the Submitting Debugging Information section for an example syntax.

The simplest first check you can do is to recompile your ASL to check for errors. Warnings can usually be ignored but errors are bugs that will usually prevent ACPI from working correctly. To recompile your ASL, issue the following command:

```
# iasl your.asl
```

33.5. Fixing Your ASL

In the long run, our goal is for almost everyone to have ACPI work without any user intervention. At this point, however, we are still developing workarounds for common mistakes made by the BIOS vendors. The Microsoft® interpreter (acpi.sys and acpiec.sys) does not strictly check for adherence to the standard, and thus many BIOS vendors who only test ACPI under Windows® never fix their ASL. We hope to continue to identify and document exactly what non-standard behavior is allowed by Microsoft®'s interpreter and replicate it so FreeBSD can work without forcing users to fix the ASL. As a workaround and to help us identify behavior, you can fix the ASL manually. If this works for you, please send a diff(1) of the old and new ASL so we can possibly work around the buggy behavior in ACPI-CA and thus make your fix unnecessary.

Here is a list of common error messages, their cause, and how to fix them:

33.5.1. _OS dependencies

Some AML assumes the world consists of various Windows® versions. You can tell FreeBSD to claim it is any OS to see if this fixes problems you may have. An easy way to override this is to set `hw.acpi.osname="Windows 2001"` in /boot/loader.conf or other similar strings you find in the ASL.

33.5.2. Missing Return statements

Some methods do not explicitly return a value as the standard requires. While ACPI-CA does not handle this, FreeBSD has a workaround that allows it to return the value implicitly. You can also add explicit Return statements where required if you know what value should be returned. To force `iasl` to compile the ASL, use the `-f` flag.

33.5.3. Overriding the Default AML

After you customize your.asl, you will want to compile it, run:

```
# iasl your.asl
```

You can add the `-f` flag to force creation of the AML, even if there are errors during compilation. Remember that some errors (e.g., missing Return statements) are automatically worked around by the interpreter.

DSDT.aml is the default output filename for `iasl`. You can load this instead of your BIOS's buggy copy (which is still present in flash memory) by editing /boot/loader.conf as follows:

```
acpi_dsdt_load="YES"
acpi_dsdt_name="/boot/DSDT.aml"
```

Be sure to copy your DSDT.aml to the /boot directory.

33.6. Getting Debugging Output From ACPI

The ACPI driver has a very flexible debugging facility. It allows you to specify a set of subsystems as well as the level of verbosity. The subsystems you wish to debug are specified as "layers" and are broken down into ACPI-CA components (ACPI_ALL_COMPONENTS) and ACPI hardware support (ACPI_ALL_DRIVERS). The verbosity of debugging output is specified as the "level" and ranges from ACPI_LV_ERROR (just report errors) to ACPI_LV_VERBOSE (everything). The "level" is a bitmask so multiple options can be set at once, separated by spaces. In practice, you will want to use a serial console to log the output if it is so long it flushes the console message buffer. A full list of the individual layers and levels is found in the acpi(4) manual page.

Debugging output is not enabled by default. To enable it, add `options ACPI_DEBUG` to your kernel configuration file if ACPI is compiled into the kernel. You can add `ACPI_DEBUG=1` to your /etc/make.conf to enable it globally. If it is a module, you can recompile just your acpi.ko module as follows:

```
# cd /sys/modules/acpi/acpi
&& make clean &&
make ACPI_DEBUG=1
```

Install acpi.ko in /boot/kernel and add your desired level and layer to loader.conf. This example enables debug messages for all ACPI-CA components and all ACPI hardware drivers (CPU, LID, etc.). It will only output error messages, the least verbose level.

```
debug.acpi.layer="ACPI_ALL_COMPONENTS ACPI_ALL_DRIVERS"
debug.acpi.level="ACPI_LV_ERROR"
```

If the information you want is triggered by a specific event (say, a suspend and then resume), you can leave out changes to loader.conf and instead use `sysctl` to specify the layer and level after booting and preparing your system for the specific event. The `sysctl`s are named the same as the tunables in loader.conf.

33.7. References

More information about ACPI may be found in the following locations:

- The ηλεκτρονική λίστα για ACPI του FreeBSD
- The ACPI Mailing List Archives http://lists.freebsd.org/pipermail/freebsd-acpi/
- The old ACPI Mailing List Archives http://home.jp.FreeBSD.org/mail-list/acpi-jp/
- The ACPI Specification
- FreeBSD Manual pages: acpi(4), acpi_thermal(4), acpidump(8), iasl(8), acpidb(8)
- DSDT debugging resource. (Uses Compaq as an example but generally useful.)

Chapter 34. Η Διαδικασία Εκκίνησης του FreeBSD

34.1. Σύνοψη

Η διαδικασία της εκκίνησης ενός υπολογιστή και φόρτωσης του λειτουργικού συστήματος αναφέρεται ως "διαδικασία bootstrap", ή απλώς "booting". Η διαδικασία εκκίνησης του FreeBSD μπορεί να προσαρμοστεί πολύ εύκολα στις απαιτήσεις σας, επιτρέποντας σάς να επιλέξετε είτε διαφορετικά λειτουργικά συστήματα που είναι εγκατεστημένα στον ίδιο υπολογιστή, ή ακόμα και διαφορετικές εκδόσεις του ίδιου λειτουργικού συστήματός ή του εγκατεστημένου πυρήνα.

Το κεφάλαιο αυτό περιγράφει λεπτομερώς τις επιλογές ρυθμίσεων που μπορείτε να κάνετε και πως να φέρετε στα μέτρα σας τη διαδικασία εκκίνησης του FreeBSD. Η διαδικασία εκκίνησης περιλαμβάνει οτιδήποτε συμβαίνει από την εκκίνηση του πυρήνα του FreeBSD, την ανίχνευση των συσκευών, μέχρι και την εκκίνηση της init(8). Η εκκίνηση της init(8) σηματοδοτείται από την αλλαγή χρώματος του κειμένου από φωτεινό λευκό σε γκρι.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Ποια είναι τα τμήματα του συστήματος εκκίνησης του FreeBSD, και πως αλληλεπιδρούν μεταξύ τους.
- Τις επιλογές που μπορείτε να δώσετε στα τμήματα της εκκίνησης του FreeBSD για να ελέγξετε τη διαδικασία εκκίνησης.
- Τα βασικά του device.hints(5).

Μόνο για υπολογιστές αρχιτεκτονικής x86

Το κεφάλαιο αυτό περιγράφει τη διαδικασία εκκίνησης του FreeBSD μόνο σε συστήματα αρχιτεκτονικής Intel x86.

34.2. Το Πρόβλημα της Εκκίνησης

Η ενεργοποίηση ενός υπολογιστή και η εκκίνηση του λειτουργικού συστήματος, μας φέρνει αντιμέτωπους με ένα ενδιαφέρον δίλημμα. Εξ' ορισμού, ο υπολογιστής δεν ξέρει να κάνει τίποτα μέχρι την εκκίνηση του λειτουργικού συστήματος. Αυτό περιλαμβάνει και την εκτέλεση προγραμμάτων από το δίσκο. Έτσι, αν ο υπολογιστής δεν μπορεί να εκτελέσει προγράμματα από το δίσκο χωρίς το λειτουργικό σύστημα, αλλά και τα προγράμματα του λειτουργικού συστήματος είναι επίσης στο δίσκο, πως είναι δυνατή η εκκίνηση του λειτουργικού;

Το πρόβλημα μοιάζει με αυτό στο βιβλίο Οι Περιπέτειες του Βαρώνου Μινχάουζεν. Ένας χαρακτήρας έχει πέσει σε ένα πηγάδι, και βγαίνει πιάνοντας και τραβώντας τα κορδόνια του (bootstraps). Στις πρώτες μέρες των υπολογιστών, χρησιμοποιούνταν ο όρος *bootstrap* για το μηχανισμό φόρτωσης του λειτουργικού συστήματος, το οποίο συντομεύτηκε σε "booting".

Στην αρχιτεκτονική x86, το Βασικό Σύστημα Εισόδου Εξόδου (BIOS) είναι υπεύθυνο για τη φόρτωση του λειτουργικού συστήματος. Για να το επιτύχει αυτό, το BIOS ανιχνεύει το σκληρό δίσκο για την

Κεντρική Εγγραφή Εκκίνησης (Master Boot Record, MBR), η οποία πρέπει να βρίσκεται σε συγκεκριμένο σημείο στο δίσκο. Το BIOS γνωρίζει αρκετά για να φορτώσει και να εκτελέσει το MBR, και υποθέτει ότι το MBR μπορεί κατόπιν να εκτελέσει την υπόλοιπη διαδικασία φόρτωσης του λειτουργικού συστήματος, ενδεχομένως και με τη βοήθεια του BIOS.

Ο κώδικας μέσα στο MBR συνήθως αναφέρεται ως *διαχειριστής εκκίνησης (boot manager)*, ειδικά όταν αλληλεπιδρά με το χρήστη. Στην περίπτωση αυτή, ο διαχειριστής εκκίνησης έχει συνήθως περισσότερο κώδικα στην πρώτη *τροχιά (track)* του δίσκου ή μέσα σε κάποιο σύστημα αρχείων του λειτουργικού. (Μερικές φορές ο διαχειριστής εκκίνησης αποκαλείται και *φορτωτής εκκίνησης (boot loader)*, αλλά στο FreeBSD ο όρος αυτός χρησιμοποιείται σε μεταγενέστερο στάδιο της εκκίνησης.) Στους δημοφιλείς διαχειριστές εκκίνησης περιλαμβάνονται το boot0 (γνωστό και ως Boot Easy, ο στάνταρ διαχειριστής εκκίνησης του FreeBSD), το Grub, το GAG, και το LILO. (Μόνο το boot0 χωράει μέσα στο MBR.)

Αν έχετε εγκατεστημένο ένα μόνο λειτουργικό σύστημα στους δίσκους σας, το τυποποιημένο MBR για PC είναι επαρκές. Αυτό το MBR ψάχνει για το πρώτο εκκινήσιμο (ή ενεργό) διαμέρισμα (slice) στο δίσκο, και εκτελεί τον κώδικα που υπάρχει σε αυτό για να φορτώσει το υπόλοιπο του λειτουργικού συστήματος. Ένα MBR αυτού του τύπου, είναι αυτό που εγκαθίσταται από προεπιλογή με την fdisk(8). Βασίζεται στο /boot/mbr.

Αν έχετε εγκαταστήσει πολλαπλά λειτουργικά συστήματα στους δίσκους σας, μπορείτε να εγκαταστήσετε διαφορετικό διαχειριστή εκκίνησης, κάποιον που να μπορεί να δείξει μια λίστα των διαφορετικών συστημάτων και να σας επιτρέψει να διαλέξετε ποιο να ξεκινήσει. Στο επόμενο τμήμα θα συζητήσουμε για δύο από αυτούς τους διαχειριστές εκκίνησης.

Το υπόλοιπο του συστήματος εκκίνησης του FreeBSD είναι χωρισμένο σε τρία στάδια. Το πρώτο στάδιο εκτελείται από το MBR, το οποίο γνωρίζει απλώς ότι απαιτείται για να φέρει τον υπολογιστή σε μια συγκεκριμένη κατάσταση και να εκτελέσει το δεύτερο στάδιο. Το δεύτερο στάδιο μπορεί να κάνει λίγα περισσότερα πράγματα πριν την εκτέλεση του τρίτου σταδίου. Το τρίτο στάδιο ολοκληρώνει τη διαδικασία φόρτωσης του λειτουργικού συστήματος. Η εργασία γίνεται σε τρία στάδια, γιατί το πρότυπο του PC επιβάλλει περιορισμούς στο μέγεθος των προγραμμάτων που μπορούν να εκτελεστούν στα στάδια ένα και δύο. Η συνένωση αυτή των εργασιών επιτρέπει στο FreeBSD να παρέχει ένα πιο ευέλικτο σύστημα φόρτωσης.

Έπειτα ξεκινάει ο πυρήνας και αρχίζει την ανίχνευση και αρχικοποίηση των συσκευών ώστε να μπορούν να χρησιμοποιηθούν. Μέτα την ολοκλήρωση της διαδικασίας εκκίνησης του πυρήνα, ο έλεγχος περνάει στη διαδικασία χρήστη init(8), η οποία και επιβεβαιώνει ότι οι δίσκοι είναι σε λειτουργική (χωρίς λάθη) κατάσταση. Η init(8) ξεκινάει έπειτα την ρύθμιση πόρων (επίπεδο χρήστη), με την οποία προσαρτώνται τα συστήματα αρχείων, ρυθμίζονται οι κάρτες δικτύου για επικοινωνία με το δίκτυο, και γενικά εκκινούν όλες οι διαδικασίες που εκτελούνται τυπικά κατά την εκκίνηση ενός FreeBSD συστήματος.

34.3. Ο Διαχειριστής Εκκίνησης και τα Στάδια Εκκίνησης

34.3.1. Ο Διαχειριστής Εκκίνησης (boot manager)

Ο κώδικας στο MBR ή διαχειριστής εκκίνησης αναφέρεται μερικές φορές και ως *στάδιο μηδέν (stage*

zero) της διαδικασίας εκκίνησης. Το τμήμα αυτό περιγράφει δύο από τους διαχειριστές εκκίνησης που αναφέραμε προηγουμένως: Το boot0 και το LILO.

Ο Διαχειριστής Εκκίνησης boot0: Το MBR που εγκαθίσταται από το πρόγραμμα εγκατάστασης του FreeBSD ή το boot0cfg(8), βασίζεται από προεπιλογή στο /boot/boot0. (Το πρόγραμμα boot0 είναι πολύ απλό, καθώς ο κώδικας στο μπορεί να έχει μέγεθος ως 446 bytes, εξαιτίας του πίνακα κατατμήσεων (slice table) και του αναγνωριστικού `0x55AA` που βρίσκεται στο τέλος του MBR.) Αν έχετε εγκαταστήσει το boot0 και πολλαπλά λειτουργικά συστήματα στους σκληρούς δίσκους σας, θα δείτε κατά την εκκίνηση, μια οθόνη παρόμοια με την παρακάτω:

Παράδειγμα 8. boot0 Screenshot

```
F1 DOS
F2 FreeBSD
F3 Linux
F4 ??
F5 Drive 1

Default: F2
```

Άλλα λειτουργικά συστήματα, και ειδικότερα τα Windows®, είναι γνωστό ότι γράφουν το δικό τους MBR πάνω σε κάποιο ήδη υπάρχον. Αν σας συμβεί αυτό, ή αν θέλετε να αντικαταστήσετε το υπάρχον MBR σας με αυτό του FreeBSD, χρησιμοποιήστε την ακόλουθη εντολή:

```
# fdisk -B -b /boot/boot0 device
```

όπου *device* είναι η συσκευή από την οποία γίνεται εκκίνηση, όπως π.χ. το ad0 για τον πρώτο δίσκο IDE, το ad2 για τον πρώτο IDE δίσκο στο δευτερεύοντα ελεγκτή, το da0 για τον πρώτο SCSI δίσκο κ.ο.κ. Αν πάλι θέλετε προσαρμοσμένη ρύθμιση του MBR, χρησιμοποιήστε το boot0cfg(8).

Ο Διαχειριστής Εκκίνησης LILO Για να εγκαταστήσετε αυτό το διαχειριστή εκκίνησης ώστε να μπορεί να εκκινεί το FreeBSD, εγκαταστήστε πρώτα το Linux και προσθέστε την ακόλουθη καταχώρηση στο υπάρχον αρχείο ρυθμίσεων /etc/lilo.conf:

```
other=/dev/hdXY
table=/dev/hdX
loader=/boot/chain.b
label=FreeBSD
```

Στο παραπάνω, καθορίστε το πρωτεύον διαμέρισμα και το δίσκο του FreeBSD αντικαθιστώντας το *X* με το γράμμα δίσκου και το *Y* με τον αριθμό του πρωτεύοντος διαμερίσματος, χρησιμοποιώντας όμως την ονοματολογία του Linux. Αν χρησιμοποιείτε οδηγό SCSI θα χρειαστεί να αλλάξετε το */dev/hd* σε κάτι αντίστοιχο με */dev/sd*. Η γραμμή `loader=/boot/chain.b` μπορεί να παραλειφθεί αν έχετε και τα δύο λειτουργικά συστήματα στον ίδιο δίσκο. Εκτελέστε τώρα την εντολή `/sbin/lilo -v` για να καταχωρήσετε τις νέες αλλαγές σας στο σύστημα. Μπορείτε να τις επιβεβαιώσετε ελέγχοντας

τα μηνύματα που θα εμφανιστούν στην οθόνη σας.

34.3.2. Το Στάδιο Ένα, /boot/boot1, και το Στάδιο Δύο, /boot/boot2

Ουσιαστικά, το πρώτο και δεύτερο στάδιο είναι τμήματα του ίδιου προγράμματος, στην ίδια περιοχή του δίσκου. Λόγω περιορισμών χώρου έχουν χωριστεί σε δύο, αλλά εγκαθίστανται πάντα μαζί. Αντιγράφονται από το συνδυασμένο αρχείο /boot/boot από το πρόγραμμα εγκατάστασης ή το bsdlabel (δείτε παρακάτω).

Βρίσκονται έξω από συστήματα αρχείων, στην πρώτη τροχιά (track) του slice εκκίνησης, ξεκινώντας από τον πρώτο τομέα. Είναι το σημείο όπου το boot0, ή οποιοσδήποτε άλλος διαχειριστής εκκίνησης, αναμένει να βρει πρόγραμμα προς εκτέλεση με το οποίο θα συνεχιστεί η διαδικασία εκκίνησης. Ο αριθμός των τομέων που χρησιμοποιούνται μπορεί να βρεθεί εύκολα από το μέγεθος του αρχείου /boot/boot.

Το boot1 είναι πολύ απλό, μια και μπορεί να είναι μόνο 512 bytes σε μέγεθος, και γνωρίζει όσα χρειάζεται για το *bsdlabel* του FreeBSD, το οποίο αποθηκεύει πληροφορίες σχετικά με το slice, ώστε να βρει και να εκτελέσει το boot2.

Το boot2 είναι ελαφρά πιο πολύπλοκο και κατανοεί επαρκώς το σύστημα αρχείων του FreeBSD ώστε να μπορεί να βρει αρχεία σε αυτό, και μπορεί επίσης να παρέχει μια απλή διεπαφή με το χρήστη ώστε να μπορεί να γίνει η επιλογή του πυρήνα ή του προγράμματος φόρτωσης που θα εκτελεστεί.

Το boot2 συνήθως εκτελεί τον loader (φορτωτής εκκίνησης) ο οποίος είναι εξαιρετικά πιο πολύπλοκος, αλλά παρέχει ένα ωραίο και εύκολο τρόπο ρύθμισης της εκκίνησης. Παλιότερα το boot2 αναλάμβανε να φορτώσει απευθείας τον πυρήνα.

Παράδειγμα 9. Εικόνα από το boot2

```
>> FreeBSD/i386 BOOT
Default: 0:ad(0,a)/boot/loader
boot:
```

Αν χρειαστεί ποτέ να αντικαταστήσετε τα εγκατεστημένα boot1 και boot2 χρησιμοποιήστε το bsdlabel(8):

```
# bsdlabel -B diskslice
```

όπου το *diskslice* είναι ο δίσκος και το slice από το οποίο γίνεται η εκκίνηση, όπως π.χ. ad0s1 για το πρώτο slice στον πρώτο IDE δίσκο.

Επικίνδυνα Αφοσιωμένη Κατάσταση (Dangerously Dedicated Mode)

Αν χρησιμοποιήσετε μόνο το όνομα του δίσκου, όπως π.χ. ad0, στην εντολή bsdlabel(8) θα δημιουργήσετε ένα επικίνδυνα αφοσιωμένο δίσκο, χωρίς slices. Είναι σχεδόν σίγουρο ότι δεν θέλετε να το κάνετε αυτό, γι' αυτό σιγουρευτείτε ότι ελέγξατε την εντολή bsdlabel(8) πριν πιέσετε `Return`.

34.3.3. Στάδιο Τρία, /boot/loader

Ο loader, ή φορτωτής εκκίνησης, είναι το τελικό στάδιο του συστήματος εκκίνησης τριών σταδίων, και βρίσκεται στο σύστημα αρχείων, συνήθως ως /boot/loader.

Προορισμός του loader είναι να παρέχει μια μέθοδο ρύθμισης φιλική προς το χρήστη, και χρησιμοποιεί ένα εύκολο σύνολο εντολών, το οποίο υποστηρίζεται από ένα ισχυρό μεταφραστή εντολών με ένα πολυπλοκότερο σύνολο εντολών.

34.3.3.1. Ροή του Προγράμματος Loader

Κατά την αρχικοποίηση, ο loader θα ανιχνεύσει την κονσόλα και τους δίσκους και θα καθορίσει από ποιο δίσκο γίνεται η εκκίνηση. Θα ρυθμίσει κατάλληλα τις αντίστοιχες μεταβλητές και θα ξεκινήσει ένα πρόγραμμα μετάφρασης εντολών (interpreter) στο οποίο μπορεί ο χρήστης να δίνει εντολές, είτε απευθείας, είτε μέσω κάποιου script.

Ο loader κατόπιν θα διαβάσει το αρχείο /boot/loader.rc, το οποίο με τη σειρά του διαβάζει, από προεπιλογή, το /boot/defaults/loader.conf. Μέσα από το αρχείο αυτό τίθενται λογικές προεπιλεγμένες τιμές για κάποιες μεταβλητές. Έπειτα, διαβάζεται το αρχείο /boot/loader.conf για τυχόν τοπικές αλλαγές στις μεταβλητές αυτές. Κατόπιν το loader.rc χρησιμοποιεί αυτές τις μεταβλητές, φορτώνοντας τα αρθρώματα (modules) και τον πυρήνα που έχει επιλεγεί.

Τελικά, ο loader, περιμένει 10 δευτερόλεπτα (προεπιλεγμένο χρονικό διάστημα) για την πίεση κάποιου πλήκτρου, και αν δεν υπάρξει παρέμβαση από τον χρήστη, ξεκινάει τον πυρήνα. Αν γίνει παρέμβαση, εμφανίζεται στον χρήστη μια προτροπή η οποίο κατανοεί το εύκολο σύνολο εντολών που αναφέραμε προηγουμένως, και όπου ο χρήστης μπορεί να ρυθμίσει μεταβλητές, να αποφορτώσει όλα τα αρθρώματα, να φορτώσει αρθρώματα και τελικά να προβεί σε εκκίνηση ή επανεκκίνηση.

34.3.3.2. Εντολές Ενσωματωμένες στο Loader

Παρακάτω θα δείτε τις πιο συχνά χρησιμοποιούμενες εντολές του loader. Για περισσότερες λεπτομέρειες σχετικά με όλες τις διαθέσιμες εντολές, παρακαλούμε να δείτε το loader(8).

autoboot ***seconds***

Προχωρά στην εκκίνηση του πυρήνα, αν δεν υπάρξει παρέμβαση από το χρήστη μέσα στο καθορισμένο χρονικό διάστημα που δίνεται σε δευτερόλεπτα. Απεικονίζει αντίστροφη μέτρηση, και ο προεπιλεγμένος χρόνος είναι τα 10 δευτερόλεπτα.

boot `[-options] [kernelname]`

Προχωράει άμεσα στην εκκίνηση του πυρήνα, χρησιμοποιώντας όποιες τυχόν επιλογές έχουν δοθεί και το όνομα του πυρήνα που θα εκτελεστεί αν έχει επίσης δοθεί. Για να δώσετε διαφορετικό όνομα πυρήνα στην γραμμή εντολής, θα πρέπει πρώτα να χρησιμοποιήσετε την εντολή *unload*. Διαφορετικά, θα χρησιμοποιηθεί ο πυρήνας που έχει φορτωθεί ήδη.

boot-conf

Διατρέχει την αυτόματη ρύθμιση των αρθρωμάτων (module) που βασίζεται σε μεταβλητές, με τον ίδιο τρόπο που γίνεται και σε κανονική εκκίνηση. Αυτό έχει νόημα μόνο αν χρησιμοποιήσετε πρώτα το `unload` και αλλάξετε κάποιες μεταβλητές, συνήθως το `kernel`.

help `[topic]`

Δείχνει μηνύματα βοήθειας, τα οποία διαβάζονται από το /boot/loader.help. Αν το topic (θέμα) που δόθηκε είναι η λέξη `index`, θα δείτε μια λίστα με τα διαθέσιμα θέματα βοήθειας.

include ***filename ...***

Επεξεργάζεται το αρχείο με το όνομα αρχείου που δόθηκε (filename). Γίνεται ανάγνωση και γραμμή προς γραμμή μετάφραση του αρχείου. Η εντολή include σταματάει άμεσα αν εντοπιστεί κάποιο λάθος.

load `[-t type]` ***filename***

Φορτώνει τον πυρήνα, το άρθρωμα πυρήνα ή ένα αρχείο του τύπου που καθορίστηκε, με βάση το όνομα αρχείου που δόθηκε. Αν μετά το όνομα αρχείου υπάρχουν παράμετροι, περνιούνται ως παράμετροι στο αρχείο που φορτώνεται.

ls `[-l] [path]`

Δείχνει ένα κατάλογο των αρχείων της διαδρομής που δόθηκε, ή αν δεν καθορίστηκε διαδρομή, του ριζικού καταλόγου. Αν δοθεί και η επιλογή `-l` θα εμφανίζονται επίσης και τα μεγέθη των αρχείων.

lsdev `[-v]`

Εμφανίζει όλες τις συσκευές από τις οποίες είναι δυνατή η φόρτωση αρθρωμάτων. Αν δοθεί με την επιλογή `-v`, εμφανίζονται περισσότερες λεπτομέρειες.

lsmod `[-v]`

Εμφανίζει τα αρθρώματα που έχουν φορτωθεί. Αν δοθεί η επιλογή `-v`, εμφανίζονται περισσότερες λεπτομέρειες.

more ***filename***

Εμφανίζει το αρχείο που καθορίζεται, με παύσεις κάθε `LINES` αριθμό γραμμών.

reboot

Επανεκκινεί άμεσα το σύστημα.

set ***variable***

Καθορίζει μεταβλητές περιβάλλοντος για τον loader.

unload

Αποφορτώνει όλα τα αρθρώματα.

34.3.3.3. Παραδείγματα για τον Loader

Εδώ θα βρείτε μερικά πρακτικά παραδείγματα σχετικά με την χρήση του loader:

- Για να ξεκινήσετε το συνηθισμένο πυρήνα σας, αλλά σε κατάσταση ενός χρήστη:

```
boot -s
```

- Για να αποφορτώσετε το συνηθισμένο πυρήνα σας και να φορτώσετε τον παλιό σας (ή κάποιο

άλλο):

```
unload
load kernel.old
```

Μπορείτε να χρησιμοποιήσετε το όνομα kernel.GENERIC για να αναφερθείτε στον αρχικό (generic) πυρήνα ο οποίος υπάρχει στο CD της εγκατάστασης, ή το kernel.old για να αναφερθείτε στον πυρήνα που είχατε εγκατεστημένο πριν (για παράδειγμα, τον παλιό σας πυρήνα αν κάνατε πρόσφατα ρύθμιση και εγκατάσταση νέου δικού σας προσαρμοσμένου πυρήνα).

Χρησιμοποιήστε το παρακάτω για να φορτώσετε τα συνηθισμένα σας αρθρώματα σε κάποιο άλλο πυρήνα:

```
unload
set kernel="kernel.old"
boot-conf
```

- Για να φορτώσετε ένα script ρύθμισης πυρήνα (ένα αυτοματοποιημένο πρόγραμμα το οποίο εκτελεί τις λειτουργίες που κανονικά θα κάνατε μέσω κάποιου προγράμματος ρύθμισης πυρήνα κατά την εκκίνηση):

```
load -t userconfig_script /boot/kernel.conf
```

34.3.3.4. Γραφική Οθόνη Εκκίνησης

Η γραφική οθόνη εκκίνησης (splash screen) δημιουργεί ένα πιο ευχάριστο περιβάλλον σε σχέση με την απλή απεικόνιση των μηνυμάτων εκκίνησης σε μορφή κειμένου. Η γραφική οθόνη εκκίνησης εμφανίζεται ως ότου το σύστημα φτάσει στην προτροπή εισόδου (login), είτε στην κονσόλα, είτε στο γραφικό περιβάλλον.

Το FreeBSD διαθέτει δύο βασικά περιβάλλοντα. Το πρώτο είναι το προεπιλεγμένο περιβάλλον κειμένου γραμμής εντολών (κονσόλα). Μετά το τέλος της εκκίνησης, εμφανίζεται στην κονσόλα μια προτροπή εισόδου. Το δεύτερο, είναι το γραφικό περιβάλλον που παρέχεται από το σύστημα X11. Μετά την εγκατάσταση του X11 και ενός από τους γραφικούς διαχειριστές παραθύρων ή desktop, όπως είναι τα GNOME, KDE ή XFce, μπορείτε να ξεκινήσετε το γραφικό περιβάλλον με την εντολή `startx`.

Μερικοί χρήστες προτιμούν να συνδέονται στο σύστημα μέσω γραφικής οθόνη εισόδου, αντί να χρησιμοποιούν την προτροπή εισόδου της κονσόλας. Η δυνατότητα αυτή παρέχεται απο διαχειριστές οθόνης, όπως ο XDM για το Xorg, ο gdm για το GNOME και ο kdm για το KDE (καθώς και άλλους που διατίθενται στη Συλλογή των Ports). Μετά από μια επιτυχημένη είσοδο, παρουσιάζεται άμεσα στο χρήστη το γραφικό περιβάλλον της επιλογής του.

Στο περιβάλλον της γραμμής εντολών, η γραφική οθόνη εκκίνησης θα αποκρύψει όλα τα μηνύματα ανίχνευσης των συσκευών και υπηρεσιών, μέχρι την εμφάνιση της προτροπής εισόδου. Με απευθείας εκκίνηση σε περιβάλλον X11, η εμπειρία εκκίνησης θα είναι ακόμα πιο καθαρή, και θα

μοιάζει περισσότερο με την αντίστοιχη σε ένα περιβάλλον Microsoft® Windows® ή άλλου μη-UNIX συστήματος.

34.3.3.4.1. Λειτουργία της Γραφικής Οθόνης Εκκίνησης

Η γραφική οθόνη εκκίνησης υποστηρίζει εικόνες bitmap (.bmp), ZSoft PCX (.pcx) ή TheDraw (.bin) 256 χρωμάτων. Επιπρόσθετα, οι εικόνες που χρησιμοποιούνται πρέπει να έχουν ανάλυση 320x200 ή μικρότερη για να λειτουργήσουν σε τυπικούς προσαρμογείς οθόνης VGA.

Για να χρησιμοποιήσετε μεγαλύτερες εικόνες, μέχρι την μέγιστη ανάλυση των 1024x768 pixels, ενεργοποιήστε την υποστήριξη VESA που περιλαμβάνεται στο FreeBSD. Μπορείτε να την ενεργοποιήσετε φορτώνοντας το άρθρωμα VESA κατά την εκκίνηση του συστήματος, η προσθέτοντας την επιλογή `VESA` στο αρχείο ρυθμίσεων του πυρήνα, και δημιουργώντας ένα νέο προσαρμοσμένο πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD). Η υποστήριξη VESA δίνει στους χρήστες την δυνατότητα να χρησιμοποιήσουν μια εικόνα που να καλύπτει όλη την οθόνη.

Μπορείτε να δείτε τα κανονικά μηνύματα εκκίνησης όσο εμφανίζεται η γραφική οθόνη εκκίνησης, πιέζοντας απλώς οποιοδήποτε πλήκτρο.

Η οθόνη εκκίνησης γίνεται επίσης η προεπιλεγμένη προφύλαξη οθόνης, όσο το σύστημα λειτουργεί σε περιβάλλον κονσόλας. Μετά από κάποιο χρονικό διάστημα αδράνειας, η οθόνη αλλάζει, απεικονίζοντας την εικόνα που χρησιμοποιήθηκε στην εκκίνηση, με κυκλική εναλλαγή της φωτεινότητας από πολύ φωτεινή ως πολύ σκοτεινή. Μπορείτε να αλλάξετε αυτή την προεπιλεγμένη προφύλαξη οθόνης, προσθέτοντας μια γραμμή `saver=` στο αρχείο /etc/rc.conf. Για την επιλογή `saver=`, υπάρχουν αρκετές ενσωματωμένες προφυλάξεις οθόνης για να επιλέξετε. Μπορείτε να δείτε την πλήρη λίστα στη σελίδα manual του splash(4). Η προεπιλεγμένη προφύλαξη οθόνης ονομάζεται "warp". Σημειώστε ότι η προφύλαξη οθόνης που καθορίζεται στο αρχείο /etc/rc.conf μέσω της επιλογής `saver=` έχει επίδραση μόνο στις εικονικές κονσόλες. Δεν επηρεάζει καθόλου το γραφικό περιβάλλον X11.

Κάποια μηνύματα εκκίνησης εξακολουθούν να εμφανίζονται, ακόμα και μετά την εφαρμογή της γραφικής οθόνης εκκίνησης. Τα μηνύματα αυτά περιλαμβάνουν το μενού επιλογών εκκίνησης και την αντίστροφη μέτρηση χρόνου που το συνοδεύει.

Μπορείτε να κατεβάσετε υποδείγματα εικόνων για χρήση στην εκκίνηση, από τη συλλογή εικόνων στην τοποθεσία http://artwork.freebsdgr.org. Αν εγκαταστήσετε το Port sysutils/bsd-splash-changer, θα έχετε τυχαία εναλλαγή εικόνων (που θα επιλέγονται από μια έτοιμη συλλογή) σε κάθε εκκίνηση του συστήματος.

34.3.3.4.2. Ενεργοποίηση της Γραφικής Οθόνης Εκκίνησης

Το αρχείο που θα χρησιμοποιηθεί για την γραφική οθόνη εκκίνησης (τύπου .bmp, .pcx ή .bin) θα πρέπει να τοποθετηθεί στην ριζική (root) κατάτμηση, για παράδειγμα στον κατάλογο /boot/.

Για την προεπιλεγμένη ανάλυση οθόνης (320x200 ή μικρότερη, 256 χρώματα), επεξεργαστείτε το αρχείο /boot/loader.conf ώστε να περιέχει τα παρακάτω:

```
splash_bmp_load="YES"
bitmap_load="YES"
```

```
bitmap_name="/boot/splash.bmp"
```

Για μεγαλύτερες αναλύσεις, μέχρι την μέγιστη 1024x768, επεξεργαστείτε το αρχείο /boot/loader.conf ώστε να περιέχει το παρακάτω:

```
vesa_load="YES"
splash_bmp_load="YES"
bitmap_load="YES"
bitmap_name="/boot/splash.bmp"
```

Το παραπάνω υποθέτει ότι θα χρησιμοποιήσετε το αρχείο /boot/splash.bmp για την γραφική οθόνη εκκίνησης. Αν θέλετε να χρησιμοποιήσετε εικόνα τύπου PCX, χρησιμοποιήστε τις παρακάτω επιλογές, καθώς και την επιλογή `vesa_load="YES"`, ανάλογα με την ανάλυση:

```
splash_pcx_load="YES"
bitmap_load="YES"
bitmap_name="/boot/splash.pcx"
```

Στην έκδοση 8.3, μια ακόμα επιλογή είναι η χρήση ascii art σε μορφή The Draw.

```
splash_txt="YES"
bitmap_load="YES"
bitmap_name="/boot/splash.bin"
```

Το όνομα αρχείου δεν είναι απαραίτητο να είναι "splash" όπως φαίνεται στο παραπάνω παράδειγμα. Μπορεί να είναι οτιδήποτε, αρκεί να πρόκειται για αρχείο των τύπων που αναφέραμε παραπάνω, για παράδειγμα splash_640x400.bmp ή blue_wave.pcx.

Παρακάτω φαίνονται μερικές ακόμα ενδιαφέρουσες επιλογές που μπορείτε να χρησιμοποιήσετε στο /boot/loader.conf:

`beastie_disable="YES"`

: Η επιλογή αυτή καταργεί την εμφάνιση του μενού επιλογών εκκίνησης. Παραμένει ωστόσο η αντίστροφη μέτρηση με την προτροπή εισαγωγής επιλογών εκκίνησης. Ακόμα και όταν δεν εμφανίζεται το μενού επιλογών, αν ο χρήστης κάνει μια επιλογή στη διάρκεια του προεπιλεγμένου χρόνου αναμονής, η επιλογή αυτή θα ισχύσει για την εκκίνηση.

`loader_logo="beastie"`

: Η επιλογή αυτή αλλάζει το κείμενο "FreeBSD" που εμφανίζεται στο δεξιό μέρος του μενού επιλογών εκκίνησης, με ένα έγχρωμο λογότυπο του beastie, όπως εμφανιζόταν στις παλαιότερες εκδόσεις.

Για περισσότερες πληροφορίες, παρακαλούμε ανατρέξτε στις σελίδες manual splash(4), loader.conf(5) και vga(4).

34.4. Αλληλεπίδραση με τον Πυρήνα κατά την Εκκίνηση

Από τη στιγμή που ο πυρήνας φορτωθεί, είτε μέσω του loader (όπως συνήθως) είτε μέσω του boot2 (παρακάμπτοντας τον loader), εξετάζει τις παραμέτρους εκκίνησης (boot flags), αν υπάρχουν, και προσαρμόζει ανάλογα τη συμπεριφορά του.

34.4.1. Παράμετροι Εκκίνησης Πυρήνα (Boot Flags)

Παρακάτω θα βρείτε τις πιο συνηθισμένες παραμέτρους εκκίνησης:

`-a`
: κατά τη διάρκεια της εκκίνησης, θα γίνει ερώτηση για την συσκευή από την οποία θα γίνει η προσάρτηση του ριζικού (root) συστήματος αρχείων.

`-C`
: εκκίνηση από το CDROM.

`-c`
: εκτέλεση του UserConfig, του προγράμματος ρύθμισης πυρήνα κατά την εκκίνηση.

`-s`
: εκκίνηση σε κατάσταση λειτουργίας ενός χρήστη (single user).

`-v`
: εμφάνιση περισσότερων πληροφοριών κατά τη διάρκεια εκκίνησης του πυρήνα.

Υπάρχουν και άλλες παράμετροι εκκίνησης, διαβάστε τη σελίδα boot(8) για περισσότερες πληροφορίες σχετικά με αυτές.

34.5. Device Hints

Κατά τη διάρκεια της αρχικής εκκίνησης του συστήματος, το πρόγραμμα του boot loader(8) διαβάζει το αρχείο device.hints(5). Το αρχείο αυτό περιέχει πληροφορίες εκκίνησης για τον πυρήνα, γνωστές ως μεταβλητές, οι οποίες μερικές φορές αναφέρονται επίσης και ως "device hints". Αυτά τα "device hints" χρησιμοποιούνται από προγράμματα οδήγησης συσκευών για ρύθμιση των αντίστοιχων συσκευών.

Μπορούμε επίσης να ορίσουμε Device hints στην προτροπή του Σταδίου 3 του boot loader. Οι μεταβλητές μπορούν να οριστούν με χρήση της εντολής `set`, και να αφαιρεθούν με την `unset`. Μπορούμε επίσης να τις εμφανίσουμε με την εντολή `show`. Ακόμα, μπορούμε εδώ να παρακάμψουμε και να αλλάξουμε την τιμή μεταβλητών που έχουν οριστεί στο αρχείο /boot/device.hints. Τα Device hints που ορίζουμε στο boot loader δεν παραμένουν μόνιμα και δεν θα ισχύσουν στην επόμενη εκκίνηση.

Μετά την εκκίνηση του συστήματος, μπορεί να χρησιμοποιηθεί η εντολή kenv(1) για να εμφανιστούν οι τιμές όλων των μεταβλητών.

Το συντακτικό του αρχείου /boot/device.hints είναι μια μεταβλητή ανά γραμμή, και χρησιμοποιείται το τυποποιημένο "#" για γραμμές που δηλώνονται ως σχόλια. Οι γραμμές δημιουργούνται όπως φαίνεται παρακάτω:

```
hint.driver.unit.keyword="value"
```

Η σύνταξη για το Στάδιο 3 του boot loader είναι:

```
set hint.driver.unit.keyword=value
```

όπου `driver` είναι το όνομα του οδηγού συσκευής, `unit` είναι ο αριθμός μονάδας της συσκευής, και `keyword` είναι η λέξη-κλειδί για το συγκεκριμένο hint. Η λέξη-κλειδί μπορεί να αποτελείται από τις ακόλουθες επιλογές:

- `at`: καθορίζει το δίαυλο (bus) στον οποίο προσαρτάται η συσκευή.
- `port`: καθορίζει την αρχική διεύθυνση της θύρας I/O που θα χρησιμοποιηθεί.
- `irq`: καθορίζει τον αριθμό της αίτησης διακοπής (interrupt request) που θα χρησιμοποιηθεί.
- `drq`: καθορίζει τον αριθμό του καναλιού DMA.
- `maddr`: καθορίζει τη φυσική διεύθυνση μνήμης που καταλαμβάνεται από τη συσκευή.
- `flags`: ορίζει διάφορα bits παραμέτρων για την συσκευή.
- `disabled`: Αν οριστεί σε τιμή 1, η συσκευή απενεργοποιείται.

Οι οδηγοί συσκευών μπορεί να δέχονται (ή να απαιτούν) περισσότερα hints τα οποία δεν φαίνονται εδώ, και σας συνιστούμε να δείτε την αντίστοιχη σελίδα manual του κάθε οδηγού. Για περισσότερες πληροφορίες συμβουλευθείτε επίσης τις σελίδες manual των device.hints(5), kenv(1), loader.conf(5), και loader(8).

34.6. Init: Αρχικοποίηση Ελέγχου Διαδικασιών

Μόλις ολοκληρωθεί η εκκίνηση του πυρήνα, ο έλεγχος μεταφέρεται στην διαδικασία χρήστη init(8), η οποία βρίσκεται στο αρχείο /sbin/init, ή στη διαδρομή που καθορίζεται στην μεταβλητή `init_path` του `loader`.

34.6.1. Ακολουθία Αυτόματης Επανεκκίνησης

Η ακολουθία αυτόματης επανεκκίνησης εξασφαλίζει ότι τα συστήματα αρχείων είναι σε κανονική, σταθερή κατάσταση. Αν δεν είναι, και η fsck(8) δεν μπορεί να διορθώσει τα προβλήματα, τότε η init(8) θα μεταφέρει το σύστημα σε κατάσταση λειτουργίας ενός χρήστη ώστε να μπορέσει άμεσα ο διαχειριστής συστήματος να επιληφθεί των προβλημάτων αυτών.

34.6.2. Κατάσταση Λειτουργίας Ενός Χρήστη

Μπορείτε να εισέλθετε στην κατάσταση αυτή μέσω της ακολουθίας αυτόματης επανεκκίνησης, ή μέσω της επιλογής `-s` κατά την εκκίνηση ή ακόμα και θέτοντας τη μεταβλητή `boot_single` στον

`loader`.

Μπορείτε επίσης να εισέλθετε σε αυτή εκτελώντας την εντολή shutdown(8) χωρίς την επιλογή επανεκκίνησης (`-r`) ή τερματισμού (`-h`), ενώ είστε σε κατάσταση λειτουργίας πολλών χρηστών (multi-user).

Αν η `κονσόλα` του συστήματος έχει τεθεί ως `insecure` (ανασφαλής) στο /etc/ttys, το σύστημα θα ζητήσει τον κωδικό του `root` πριν εισέλθει σε κατάσταση λειτουργίας ενός χρήστη.

Παράδειγμα 10. Ανασφαλής Κονσόλα στο /etc/ttys

```
# name  getty                           type    status          comments
#
# If console is marked "insecure", then init will ask for the root password
# when going to single-user mode.
console none                            unknown off insecure
```

Μια `insecure` (ανασφαλής) κονσόλα σημαίνει ότι δεν θεωρείτε ασφαλή την κονσόλα όσο αφορά τη φυσική της πρόσβαση και θέλετε να είστε βέβαιος ότι μόνο όποιος γνωρίζει τον κωδικό του `root` θα μπορεί να χρησιμοποιήσει τη λειτουργία ενός χρήστη. Η επιλογή αυτή δεν σημαίνει ότι θέλετε η κονσόλα σας να λειτουργεί χωρίς ασφάλεια. Αν θέλετε ασφάλεια, θα πρέπει να επιλέξετε `insecure`, όχι `secure`.

34.6.3. Κατάσταση Λειτουργία Πολλαπλών Χρηστών (multi-user)

Αν η init(8) δεν βρει προβλήματα στα συστήματα αρχείων σας, ή μόλις ο χρήστης τερματίσει την κατάσταση λειτουργίας ενός χρήστη, το σύστημα εισέρχεται σε λειτουργία πολλαπλών χρηστών, όπου και ξεκινά πλέον η ρύθμιση πόρων (resources) του συστήματος.

34.6.3.1. Ρύθμιση Πόρων (rc)

Το σύστημα ρύθμισης πόρων, διαβάζει τις προεπιλεγμένες επιλογές από το /etc/defaults/rc.conf, και επιλογές για το συγκεκριμένο μηχάνημα από το /etc/rc.conf, και προχωρεί στην προσάρτηση των συστημάτων αρχείων που αναγράφονται στο /etc/fstab, ξεκινά τις υπηρεσίες δικτύου, εκκινεί διάφορους δαίμονες, και τέλος εκτελεί τα scripts εκκίνησης των τοπικά εγκατεστημένων πακέτων (εφαρμογών).

Η σελίδα manual rc(8) παρέχει μια καλή αναφορά στο σύστημα ρύθμισης πόρων, καθώς εξετάζει τα ίδια τα scripts εκκίνησης.

34.7. Ακολουθία Τερματισμού

Κατά τον ελεγχόμενο τερματισμό, μέσω της shutdown(8), η init(8) θα αποπειραθεί να εκτελέσει το script /etc/rc.shutdown, και ακολούθως θα στείλει σε όλες τις διεργασίες το σήμα `TERM`, και τέλος το σήμα `KILL` σε όποια διεργασία δεν τερματίσει σε εύλογο χρονικό διάστημα.

Για να γίνει και διακοπή της τροφοδοσίας σε ένα σύστημα FreeBSD με αρχιτεκτονική που

υποστηρίζει διαχείριση ενέργειας, απλώς χρησιμοποιήστε την εντολή `shutdown -p now` για απενεργοποίηση μετά τον τερματισμό. Για να κάνετε απλώς επανεκκίνηση σε ένα σύστημα FreeBSD χρησιμοποιήστε την εντολή `shutdown -r now`. Θα πρέπει να είστε `root` ή μέλος της ομάδας `operator` για να εκτελέσετε την shutdown(8). Μπορείτε επίσης να χρησιμοποιήσετε τις εντολές halt(8) και reboot(8), κοιτάξτε τις αντίστοιχες σελίδες manual καθώς και τη σελίδα manual της shutdown(8) για περισσότερες πληροφορίες.

Η διαχείριση ενέργειας απαιτεί την υποστήριξη του acpi(4), είτε στον πυρήνα, είτε φορτωμένη ως άρθρωμα (module).

Chapter 35. Ασφάλεια

35.1. Σύνοψη

Το κεφάλαιο αυτό παρέχει μια βασική εισαγωγή στις έννοιες της ασφάλειας συστήματος, κάποιους γενικά καλούς κανόνες, και ορισμένα προχωρημένα θέματα σχετικά με το FreeBSD. Αρκετά από τα θέματα που καλύπτονται εδώ, μπορούν να εφαρμοστούν το ίδιο καλά τόσο στο ίδιο το σύστημα, όσο και για ασφάλεια μέσω Internet. Το Internet δεν είναι πλέον ένα "φιλικό" μέρος στο οποίο καθένας θέλει να είναι ο ευγενικός σας γείτονας. Η ανάγκη ασφάλισης του συστήματος σας είναι επιτακτική για να προστατέψετε τα δεδομένα σας,την πνευματική σας ιδιοκτησία, το χρόνο σας, και πολλά περισσότερα από τα χέρια των χάκερς και των ομοίων τους.

Το FreeBSD παρέχει μια σειρά από βοηθητικά προγράμματα και μηχανισμούς για να εξασφαλίσει την ακεραιότητα και την ασφάλεια του συστήματος σας και του δικτύου.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Βασικές έννοιες για την ασφάλεια, σε σχέση με το FreeBSD.
- Στοιχεία σχετικά με τους διάφορους μηχανισμούς κρυπτογράφησης που είναι διαθέσιμοι στο FreeBSD, όπως το DES και το MD5.
- Πως να ρυθμίσετε το σύστημα σας για κωδικούς μιας χρήσης.
- Πως να ρυθμίσετε TCP Wrappers για χρήση με την `inetd`.
- Πως να ρυθμίσετε τον KerberosIV σε FreeBSD εκδόσεις πριν τη 5.0.
- Πως να ρυθμίσετε τον Kerberos5 στο FreeBSD.
- Πως να ρυθμίσετε το IPsec και να δημιουργήσετε ένα VPN μεταξύ μηχανημάτων FreeBSD/Windows®.
- Πως να ρυθμίσετε και να χρησιμοποιήσετε την κατά FreeBSD υλοποίηση SSH του OpenSSH
- Τι είναι τα ACLs στο σύστημα αρχείων και πως να τα χρησιμοποιήσετε.
- Πως να χρησιμοποιήσετε το βοηθητικό πρόγραμμα Portaudit για να ελέγξετε λογισμικό τρίτου κατασκευαστή που έχει εγκατασταθεί μέσω της συλλογής Ports.
- Πως να χρησιμοποιήσετε τις δημοσιεύσεις security advisories του FreeBSD.
- Θα έχετε μια ιδέα για το τι είναι το Process Accounting και πως να το ενεργοποιήσετε στο FreeBSD.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε βασικές έννοιες του FreeBSD και του Internet.

Πρόσθετα θέματα σχετικά με την ασφάλεια καλύπτονται σε ολόκληρο το βιβλίο. Για παράδειγμα, ο Υποχρεωτικός Έλεγχος Πρόσβασης συζητείται στο Υποχρεωτικός Έλεγχος Πρόσβασης και τα Internet Firewalls συζητούνται στο Firewalls.

35.2. Introduction

Security is a function that begins and ends with the system administrator. While all BSD UNIX® multi-user systems have some inherent security, the job of building and maintaining additional security mechanisms to keep those users "honest" is probably one of the single largest undertakings of the sysadmin. Machines are only as secure as you make them, and security concerns are ever competing with the human necessity for convenience. UNIX® systems, in general, are capable of running a huge number of simultaneous processes and many of these processes operate as servers - meaning that external entities can connect and talk to them. As yesterday's mini-computers and mainframes become today's desktops, and as computers become networked and inter-networked, security becomes an even bigger issue.

System security also pertains to dealing with various forms of attack, including attacks that attempt to crash, or otherwise make a system unusable, but do not attempt to compromise the `root` account ("break root"). Security concerns can be split up into several categories:

1. Denial of service attacks.
2. User account compromises.
3. Root compromise through accessible servers.
4. Root compromise via user accounts.
5. Backdoor creation.

A denial of service attack is an action that deprives the machine of needed resources. Typically, DoS attacks are brute-force mechanisms that attempt to crash or otherwise make a machine unusable by overwhelming its servers or network stack. Some DoS attacks try to take advantage of bugs in the networking stack to crash a machine with a single packet. The latter can only be fixed by applying a bug fix to the kernel. Attacks on servers can often be fixed by properly specifying options to limit the load the servers incur on the system under adverse conditions. Brute-force network attacks are harder to deal with. A spoofed-packet attack, for example, is nearly impossible to stop, short of cutting your system off from the Internet. It may not be able to take your machine down, but it can saturate your Internet connection.

A user account compromise is even more common than a DoS attack. Many sysadmins still run standard telnetd, rlogind, rshd, and ftpd servers on their machines. These servers, by default, do not operate over encrypted connections. The result is that if you have any moderate-sized user base, one or more of your users logging into your system from a remote location (which is the most common and convenient way to login to a system) will have his or her password sniffed. The attentive system admin will analyze his remote access logs looking for suspicious source addresses even for successful logins.

One must always assume that once an attacker has access to a user account, the attacker can break `root`. However, the reality is that in a well secured and maintained system, access to a user account does not necessarily give the attacker access to `root`. The distinction is important because without access to `root` the attacker cannot generally hide his tracks and may, at best, be able to do nothing more than mess with the user's files, or crash the machine. User account compromises are very common because users tend not to take the precautions that sysadmins take.

System administrators must keep in mind that there are potentially many ways to break `root` on a machine. The attacker may know the `root` password, the attacker may find a bug in a root-run server and be able to break `root` over a network connection to that server, or the attacker may know of a bug in a suid-root program that allows the attacker to break `root` once he has broken into a user's account. If an attacker has found a way to break `root` on a machine, the attacker may not have a need to install a backdoor. Many of the `root` holes found and closed to date involve a considerable amount of work by the attacker to cleanup after himself, so most attackers install backdoors. A backdoor provides the attacker with a way to easily regain `root` access to the system, but it also gives the smart system administrator a convenient way to detect the intrusion. Making it impossible for an attacker to install a backdoor may actually be detrimental to your security, because it will not close off the hole the attacker found to break in the first place.

Security remedies should always be implemented with a multi-layered "onion peel" approach and can be categorized as follows:

1. Securing `root` and staff accounts.
2. Securing `root`-run servers and suid/sgid binaries.
3. Securing user accounts.
4. Securing the password file.
5. Securing the kernel core, raw devices, and file systems.
6. Quick detection of inappropriate changes made to the system.
7. Paranoia.

The next section of this chapter will cover the above bullet items in greater depth.

35.3. Securing FreeBSD

Command vs. Protocol

Throughout this document, we will use bold text to refer to an application, and a `monospaced` font to refer to specific commands. Protocols will use a normal font. This typographical distinction is useful for instances such as ssh, since it is a protocol as well as command.

The sections that follow will cover the methods of securing your FreeBSD system that were mentioned in the last section of this chapter.

35.3.1. Securing the `root` Account and Staff Accounts

First off, do not bother securing staff accounts if you have not secured the `root` account. Most systems have a password assigned to the `root` account. The first thing you do is assume that the password is *always* compromised. This does not mean that you should remove the password. The password is almost always necessary for console access to the machine. What it does mean is that you should not make it possible to use the password outside of the console or possibly even with the su(1) command. For example, make sure that your ptys are specified as being insecure in the /etc/ttys file so that direct `root` logins via `telnet` or `rlogin` are disallowed. If using other login

services such as sshd, make sure that direct `root` logins are disabled there as well. You can do this by editing your /etc/ssh/sshd_config file, and making sure that `PermitRootLogin` is set to `NO`. Consider every access method - services such as FTP often fall through the cracks. Direct `root` logins should only be allowed via the system console.

Of course, as a sysadmin you have to be able to get to `root`, so we open up a few holes. But we make sure these holes require additional password verification to operate. One way to make `root` accessible is to add appropriate staff accounts to the `wheel` group (in /etc/group). The staff members placed in the `wheel` group are allowed to `su` to `root`. You should never give staff members native `wheel` access by putting them in the `wheel` group in their password entry. Staff accounts should be placed in a `staff` group, and then added to the `wheel` group via the /etc/group file. Only those staff members who actually need to have `root` access should be placed in the `wheel` group. It is also possible, when using an authentication method such as Kerberos, to use Kerberos' .k5login file in the `root` account to allow a ksu(1) to `root` without having to place anyone at all in the `wheel` group. This may be the better solution since the `wheel` mechanism still allows an intruder to break `root` if the intruder has gotten hold of your password file and can break into a staff account. While having the `wheel` mechanism is better than having nothing at all, it is not necessarily the safest option.

An indirect way to secure staff accounts, and ultimately `root` access is to use an alternative login access method and do what is known as "starring" out the encrypted password for the staff accounts. Using the vipw(8) command, one can replace each instance of an encrypted password with a single “*” character. This command will update the /etc/master.passwd file and user/password database to disable password-authenticated logins.

A staff account entry such as:

```
foobar:R9DT/Fa1/LV9U:1000:1000::0:0:Foo Bar:/home/foobar:/usr/local/bin/tcsh
```

Should be changed to this:

```
foobar:*:1000:1000::0:0:Foo Bar:/home/foobar:/usr/local/bin/tcsh
```

This change will prevent normal logins from occurring, since the encrypted password will never match “*”. With this done, staff members must use another mechanism to authenticate themselves such as kerberos(1) or ssh(1) using a public/private key pair. When using something like Kerberos, one generally must secure the machines which run the Kerberos servers and your desktop workstation. When using a public/private key pair with ssh, one must generally secure the machine used to login *from* (typically one’s workstation). An additional layer of protection can be added to the key pair by password protecting the key pair when creating it with ssh-keygen(1). Being able to "star" out the passwords for staff accounts also guarantees that staff members can only login through secure access methods that you have set up. This forces all staff members to use secure, encrypted connections for all of their sessions, which closes an important hole used by many intruders: sniffing the network from an unrelated, less secure machine.

The more indirect security mechanisms also assume that you are logging in from a more restrictive server to a less restrictive server. For example, if your main box is running all sorts of servers, your workstation should not be running any. In order for your workstation to be reasonably secure you

should run as few servers as possible, up to and including no servers at all, and you should run a password-protected screen blanker. Of course, given physical access to a workstation an attacker can break any sort of security you put on it. This is definitely a problem that you should consider, but you should also consider the fact that the vast majority of break-ins occur remotely, over a network, from people who do not have physical access to your workstation or servers.

Using something like Kerberos also gives you the ability to disable or change the password for a staff account in one place, and have it immediately affect all the machines on which the staff member may have an account. If a staff member's account gets compromised, the ability to instantly change his password on all machines should not be underrated. With discrete passwords, changing a password on N machines can be a mess. You can also impose re-passwording restrictions with Kerberos: not only can a Kerberos ticket be made to timeout after a while, but the Kerberos system can require that the user choose a new password after a certain period of time (say, once a month).

35.3.2. Securing Root-run Servers and SUID/SGID Binaries

The prudent sysadmin only runs the servers he needs to, no more, no less. Be aware that third party servers are often the most bug-prone. For example, running an old version of imapd or popper is like giving a universal `root` ticket out to the entire world. Never run a server that you have not checked out carefully. Many servers do not need to be run as `root`. For example, the ntalk, comsat, and finger daemons can be run in special user *sandboxes*. A sandbox is not perfect, unless you go through a large amount of trouble, but the onion approach to security still stands: If someone is able to break in through a server running in a sandbox, they still have to break out of the sandbox. The more layers the attacker must break through, the lower the likelihood of his success. Root holes have historically been found in virtually every server ever run as `root`, including basic system servers. If you are running a machine through which people only login via sshd and never login via telnetd or rshd or rlogind, then turn off those services!

FreeBSD now defaults to running ntalkd, comsat, and finger in a sandbox. Another program which may be a candidate for running in a sandbox is named(8). /etc/defaults/rc.conf includes the arguments necessary to run named in a sandbox in a commented-out form. Depending on whether you are installing a new system or upgrading an existing system, the special user accounts used by these sandboxes may not be installed. The prudent sysadmin would research and implement sandboxes for servers whenever possible.

There are a number of other servers that typically do not run in sandboxes: sendmail, popper, imapd, ftpd, and others. There are alternatives to some of these, but installing them may require more work than you are willing to perform (the convenience factor strikes again). You may have to run these servers as `root` and rely on other mechanisms to detect break-ins that might occur through them.

The other big potential `root` holes in a system are the suid-root and sgid binaries installed on the system. Most of these binaries, such as rlogin, reside in /bin, /sbin, /usr/bin, or /usr/sbin. While nothing is 100% safe, the system-default suid and sgid binaries can be considered reasonably safe. Still, `root` holes are occasionally found in these binaries. A `root` hole was found in `Xlib` in 1998 that made xterm (which is typically suid) vulnerable. It is better to be safe than sorry and the prudent sysadmin will restrict suid binaries, that only staff should run, to a special group that only staff can access, and get rid of (`chmod 000`) any suid binaries that nobody uses. A server with no display

generally does not need an xterm binary. Sgid binaries can be almost as dangerous. If an intruder can break an sgid-kmem binary, the intruder might be able to read /dev/kmem and thus read the encrypted password file, potentially compromising any passworded account. Alternatively an intruder who breaks group `kmem` can monitor keystrokes sent through ptys, including ptys used by users who login through secure methods. An intruder that breaks the `tty` group can write to almost any user's tty. If a user is running a terminal program or emulator with a keyboard-simulation feature, the intruder can potentially generate a data stream that causes the user's terminal to echo a command, which is then run as that user.

35.3.3. Securing User Accounts

User accounts are usually the most difficult to secure. While you can impose draconian access restrictions on your staff and "star" out their passwords, you may not be able to do so with any general user accounts you might have. If you do have sufficient control, then you may win out and be able to secure the user accounts properly. If not, you simply have to be more vigilant in your monitoring of those accounts. Use of ssh and Kerberos for user accounts is more problematic, due to the extra administration and technical support required, but still a very good solution compared to a encrypted password file.

35.3.4. Securing the Password File

The only sure fire way is to star out as many passwords as you can and use ssh or Kerberos for access to those accounts. Even though the encrypted password file (/etc/spwd.db) can only be read by `root`, it may be possible for an intruder to obtain read access to that file even if the attacker cannot obtain root-write access.

Your security scripts should always check for and report changes to the password file (see the Checking file integrity section below).

35.3.5. Securing the Kernel Core, Raw Devices, and File systems

If an attacker breaks `root` he can do just about anything, but there are certain conveniences. For example, most modern kernels have a packet sniffing device driver built in. Under FreeBSD it is called the bpf device. An intruder will commonly attempt to run a packet sniffer on a compromised machine. You do not need to give the intruder the capability and most systems do not have the need for the bpf device compiled in.

But even if you turn off the bpf device, you still have /dev/mem and /dev/kmem to worry about. For that matter, the intruder can still write to raw disk devices. Also, there is another kernel feature called the module loader, kldload(8). An enterprising intruder can use a KLD module to install his own bpf device, or other sniffing device, on a running kernel. To avoid these problems you have to run the kernel at a higher secure level, at least securelevel 1. The securelevel can be set with a `sysctl` on the `kern.securelevel` variable. Once you have set the securelevel to 1, write access to raw devices will be denied and special `chflags` flags, such as `schg`, will be enforced. You must also ensure that the `schg` flag is set on critical startup binaries, directories, and script files - everything that gets run up to the point where the securelevel is set. This might be overdoing it, and upgrading the system is much more difficult when you operate at a higher secure level. You may compromise and run the system at a higher secure level but not set the `schg` flag for every system file and directory

under the sun. Another possibility is to simply mount / and /usr read-only. It should be noted that being too draconian in what you attempt to protect may prevent the all-important detection of an intrusion.

35.3.6. Checking File Integrity: Binaries, Configuration Files, Etc.

When it comes right down to it, you can only protect your core system configuration and control files so much before the convenience factor rears its ugly head. For example, using `chflags` to set the `schg` bit on most of the files in / and /usr is probably counterproductive, because while it may protect the files, it also closes a detection window. The last layer of your security onion is perhaps the most important - detection. The rest of your security is pretty much useless (or, worse, presents you with a false sense of security) if you cannot detect potential intrusions. Half the job of the onion is to slow down the attacker, rather than stop him, in order to be able to catch him in the act.

The best way to detect an intrusion is to look for modified, missing, or unexpected files. The best way to look for modified files is from another (often centralized) limited-access system. Writing your security scripts on the extra-secure limited-access system makes them mostly invisible to potential attackers, and this is important. In order to take maximum advantage you generally have to give the limited-access box significant access to the other machines in the business, usually either by doing a read-only NFS export of the other machines to the limited-access box, or by setting up ssh key-pairs to allow the limited-access box to ssh to the other machines. Except for its network traffic, NFS is the least visible method - allowing you to monitor the file systems on each client box virtually undetected. If your limited-access server is connected to the client boxes through a switch, the NFS method is often the better choice. If your limited-access server is connected to the client boxes through a hub, or through several layers of routing, the NFS method may be too insecure (network-wise) and using ssh may be the better choice even with the audit-trail tracks that ssh lays.

Once you have given a limited-access box at least read access to the client systems it is supposed to monitor, you must write scripts to do the actual monitoring. Given an NFS mount, you can write scripts out of simple system utilities such as find(1) and md5(1). It is best to physically md5 the client-box files at least once a day, and to test control files such as those found in /etc and /usr/local/etc even more often. When mismatches are found, relative to the base md5 information the limited-access machine knows is valid, it should scream at a sysadmin to go check it out. A good security script will also check for inappropriate suid binaries and for new or deleted files on system partitions such as / and /usr.

When using ssh rather than NFS, writing the security script is much more difficult. You essentially have to `scp` the scripts to the client box in order to run them, making them visible, and for safety you also need to `scp` the binaries (such as find) that those scripts use. The ssh client on the client box may already be compromised. All in all, using ssh may be necessary when running over insecure links, but it is also a lot harder to deal with.

A good security script will also check for changes to user and staff members access configuration files: .rhosts, .shosts, .ssh/authorized_keys and so forth, files that might fall outside the purview of the `MD5` check.

If you have a huge amount of user disk space, it may take too long to run through every file on those partitions. In this case, setting mount flags to disallow suid binaries and devices on those partitions is a good idea. The `nodev` and `nosuid` options (see mount(8)) are what you want to look

into. You should probably scan them anyway, at least once a week, since the object of this layer is to detect a break-in attempt, whether or not the attempt succeeds.

Process accounting (see accton(8)) is a relatively low-overhead feature of the operating system which might help as a post-break-in evaluation mechanism. It is especially useful in tracking down how an intruder has actually broken into a system, assuming the file is still intact after the break-in has occurred.

Finally, security scripts should process the log files, and the logs themselves should be generated in as secure a manner as possible - remote syslog can be very useful. An intruder will try to cover his tracks, and log files are critical to the sysadmin trying to track down the time and method of the initial break-in. One way to keep a permanent record of the log files is to run the system console to a serial port and collect the information to a secure machine monitoring the consoles.

35.3.7. Paranoia

A little paranoia never hurts. As a rule, a sysadmin can add any number of security features, as long as they do not affect convenience, and can add security features that *do* affect convenience with some added thought. Even more importantly, a security administrator should mix it up a bit - if you use recommendations such as those given by this document verbatim, you give away your methodologies to the prospective attacker who also has access to this document.

35.3.8. Denial of Service Attacks

This section covers Denial of Service attacks. A DoS attack is typically a packet attack. While there is not much you can do about modern spoofed packet attacks that saturate your network, you can generally limit the damage by ensuring that the attacks cannot take down your servers by:

1. Limiting server forks.
2. Limiting springboard attacks (ICMP response attacks, ping broadcast, etc.).
3. Overloading the Kernel Route Cache.

A common DoS attack scenario is attacking a forking server and making it spawning so many child processes that the host system eventually runs out of memory, file descriptors, etc. and then grinds to a halt. inetd (see inetd(8)) has several options to limit this sort of attack. It should be noted that while it is possible to prevent a machine from going down, it is not generally possible to prevent a service from being disrupted by the attack. Read the inetd manual page carefully and pay specific attention to the `-c`, `-C`, and `-R` options. Note that spoofed-IP attacks will circumvent the `-C` option to inetd, so typically a combination of options must be used. Some standalone servers have self-fork-limitation parameters.

Sendmail has its `-OMaxDaemonChildren` option, which tends to work much better than trying to use Sendmail's load limiting options due to the load lag. You should specify a `MaxDaemonChildren` parameter, when you start sendmail; high enough to handle your expected load, but not so high that the computer cannot handle that number of Sendmail instances without falling on its face. It is also prudent to run Sendmail in queued mode (`-ODeliveryMode=queued`) and to run the daemon (`sendmail -bd`) separate from the queue-runs (`sendmail -q15m`). If you still want real-time delivery you can run the queue at a much lower interval, such as `-q1m`, but be sure to specify a reasonable

`MaxDaemonChildren` option for *that* Sendmail to prevent cascade failures.

Syslogd can be attacked directly and it is strongly recommended that you use the `-s` option whenever possible, and the `-a` option otherwise.

You should also be fairly careful with connect-back services such as TCP Wrapper's reverse-identd, which can be attacked directly. You generally do not want to use the reverse-ident feature of TCP Wrapper for this reason.

It is a very good idea to protect internal services from external access by firewalling them off at your border routers. The idea here is to prevent saturation attacks from outside your LAN, not so much to protect internal services from network-based `root` compromise. Always configure an exclusive firewall, i.e., "firewall everything *except* ports A, B, C, D, and M-Z". This way you can firewall off all of your low ports except for certain specific services such as named (if you are primary for a zone), ntalkd, sendmail, and other Internet-accessible services. If you try to configure the firewall the other way - as an inclusive or permissive firewall, there is a good chance that you will forget to "close" a couple of services, or that you will add a new internal service and forget to update the firewall. You can still open up the high-numbered port range on the firewall, to allow permissive-like operation, without compromising your low ports. Also take note that FreeBSD allows you to control the range of port numbers used for dynamic binding, via the various `net.inet.ip.portrange sysctl`'s (`sysctl -a | fgrep portrange`), which can also ease the complexity of your firewall's configuration. For example, you might use a normal first/last range of 4000 to 5000, and a hiport range of 49152 to 65535, then block off everything under 4000 in your firewall (except for certain specific Internet-accessible ports, of course).

Another common DoS attack is called a springboard attack - to attack a server in a manner that causes the server to generate responses which overloads the server, the local network, or some other machine. The most common attack of this nature is the *ICMP ping broadcast attack*. The attacker spoofs ping packets sent to your LAN's broadcast address with the source IP address set to the actual machine they wish to attack. If your border routers are not configured to stomp on ping packets to broadcast addresses, your LAN winds up generating sufficient responses to the spoofed source address to saturate the victim, especially when the attacker uses the same trick on several dozen broadcast addresses over several dozen different networks at once. Broadcast attacks of over a hundred and twenty megabits have been measured. A second common springboard attack is against the ICMP error reporting system. By constructing packets that generate ICMP error responses, an attacker can saturate a server's incoming network and cause the server to saturate its outgoing network with ICMP responses. This type of attack can also crash the server by running it out of memory, especially if the server cannot drain the ICMP responses it generates fast enough. Use the sysctl variable `net.inet.icmp.icmplim` to limit these attacks. The last major class of springboard attacks is related to certain internal inetd services such as the udp echo service. An attacker simply spoofs a UDP packet with the source address being server A's echo port, and the destination address being server B's echo port, where server A and B are both on your LAN. The two servers then bounce this one packet back and forth between each other. The attacker can overload both servers and their LANs simply by injecting a few packets in this manner. Similar problems exist with the internal chargen port. A competent sysadmin will turn off all of these inetd-internal test services.

Spoofed packet attacks may also be used to overload the kernel route cache. Refer to the `net.inet.ip.rtexpire`, `rtminexpire`, and `rtmaxcache sysctl` parameters. A spoofed packet attack that

uses a random source IP will cause the kernel to generate a temporary cached route in the route table, viewable with `netstat -rna | fgrep W3`. These routes typically timeout in 1600 seconds or so. If the kernel detects that the cached route table has gotten too big it will dynamically reduce the `rtexpire` but will never decrease it to less than `rtminexpire`. There are two problems:

1. The kernel does not react quickly enough when a lightly loaded server is suddenly attacked.
2. The `rtminexpire` is not low enough for the kernel to survive a sustained attack.

If your servers are connected to the Internet via a T3 or better, it may be prudent to manually override both `rtexpire` and `rtminexpire` via sysctl(8). Never set either parameter to zero (unless you want to crash the machine). Setting both parameters to 2 seconds should be sufficient to protect the route table from attack.

35.3.9. Access Issues with Kerberos and SSH

There are a few issues with both Kerberos and ssh that need to be addressed if you intend to use them. Kerberos 5 is an excellent authentication protocol, but there are bugs in the kerberized telnet and rlogin applications that make them unsuitable for dealing with binary streams. Also, by default Kerberos does not encrypt a session unless you use the `-x` option. ssh encrypts everything by default.

Ssh works quite well in every respect except that it forwards encryption keys by default. What this means is that if you have a secure workstation holding keys that give you access to the rest of the system, and you ssh to an insecure machine, your keys are usable. The actual keys themselves are not exposed, but ssh installs a forwarding port for the duration of your login, and if an attacker has broken `root` on the insecure machine he can utilize that port to use your keys to gain access to any other machine that your keys unlock.

We recommend that you use ssh in combination with Kerberos whenever possible for staff logins. Ssh can be compiled with Kerberos support. This reduces your reliance on potentially exposed ssh keys while at the same time protecting passwords via Kerberos. Ssh keys should only be used for automated tasks from secure machines (something that Kerberos is unsuited to do). We also recommend that you either turn off key-forwarding in the ssh configuration, or that you make use of the `from=IP/DOMAIN` option that ssh allows in its authorized_keys file to make the key only usable to entities logging in from specific machines.

35.4. DES, MD5, and Crypt

Every user on a UNIX® system has a password associated with their account. It seems obvious that these passwords need to be known only to the user and the actual operating system. In order to keep these passwords secret, they are encrypted with what is known as a "one-way hash", that is, they can only be easily encrypted but not decrypted. In other words, what we told you a moment ago was obvious is not even true: the operating system itself does not *really* know the password. It only knows the *encrypted* form of the password. The only way to get the "plain-text" password is by a brute force search of the space of possible passwords.

Unfortunately the only secure way to encrypt passwords when UNIX® came into being was based on DES, the Data Encryption Standard. This was not such a problem for users resident in the US, but

since the source code for DES could not be exported outside the US, FreeBSD had to find a way to both comply with US law and retain compatibility with all the other UNIX® variants that still used DES.

The solution was to divide up the encryption libraries so that US users could install the DES libraries and use DES but international users still had an encryption method that could be exported abroad. This is how FreeBSD came to use MD5 as its default encryption method. MD5 is believed to be more secure than DES, so installing DES is offered primarily for compatibility reasons.

35.4.1. Recognizing Your Crypt Mechanism

Currently the library supports DES, MD5 and Blowfish hash functions. By default FreeBSD uses MD5 to encrypt passwords.

It is pretty easy to identify which encryption method FreeBSD is set up to use. Examining the encrypted passwords in the /etc/master.passwd file is one way. Passwords encrypted with the MD5 hash are longer than those encrypted with the DES hash and also begin with the characters `$1$`. Passwords starting with `$2a$` are encrypted with the Blowfish hash function. DES password strings do not have any particular identifying characteristics, but they are shorter than MD5 passwords, and are coded in a 64-character alphabet which does not include the `$` character, so a relatively short string which does not begin with a dollar sign is very likely a DES password.

The password format used for new passwords is controlled by the `passwd_format` login capability in /etc/login.conf, which takes values of `des`, `md5` or `blf`. See the login.conf(5) manual page for more information about login capabilities.

35.5. One-time Passwords

By default, FreeBSD includes support for OPIE (One-time Passwords In Everything), which uses the MD5 hash by default.

There are three different sorts of passwords which we will discuss below. The first is your usual UNIX® style or Kerberos password; we will call this a "UNIX® password". The second sort is the one-time password which is generated by the OPIE opiekey(1) program and accepted by the opiepasswd(1) program and the login prompt; we will call this a "one-time password". The final sort of password is the secret password which you give to the `opiekey` program (and sometimes the `opiepasswd` programs) which it uses to generate one-time passwords; we will call it a "secret password" or just unqualified "password".

The secret password does not have anything to do with your UNIX® password; they can be the same but this is not recommended. OPIE secret passwords are not limited to 8 characters like old UNIX® passwords, they can be as long as you like. Passwords of six or seven word long phrases are fairly common. For the most part, the OPIE system operates completely independently of the UNIX® password system.

Besides the password, there are two other pieces of data that are important to OPIE. One is what is known as the "seed" or "key", consisting of two letters and five digits. The other is what is called the "iteration count", a number between 1 and 100. OPIE creates the one-time password by concatenating the seed and the secret password, then applying the MD5 hash as many times as

specified by the iteration count and turning the result into six short English words. These six English words are your one-time password. The authentication system (primarily PAM) keeps track of the last one-time password used, and the user is authenticated if the hash of the user-provided password is equal to the previous password. Because a one-way hash is used it is impossible to generate future one-time passwords if a successfully used password is captured; the iteration count is decremented after each successful login to keep the user and the login program in sync. When the iteration count gets down to 1, OPIE must be reinitialized.

There are a few programs involved in each system which we will discuss below. The `opiekey` program accepts an iteration count, a seed, and a secret password, and generates a one-time password or a consecutive list of one-time passwords. The `opiepasswd` program is used to initialize OPIE, and to change passwords, iteration counts, or seeds; it takes either a secret passphrase, or an iteration count, seed, and a one-time password. The `opieinfo` program will examine the relevant credentials files (/etc/opiekeys) and print out the invoking user's current iteration count and seed.

There are four different sorts of operations we will cover. The first is using `opiepasswd` over a secure connection to set up one-time-passwords for the first time, or to change your password or seed. The second operation is using `opiepasswd` over an insecure connection, in conjunction with `opiekey` over a secure connection, to do the same. The third is using `opiekey` to log in over an insecure connection. The fourth is using `opiekey` to generate a number of keys which can be written down or printed out to carry with you when going to some location without secure connections to anywhere.

35.5.1. Secure Connection Initialization

To initialize OPIE for the first time, execute the `opiepasswd` command:

```
% opiepasswd -c
[grimreaper] ~ $ opiepasswd -f -c
Adding unfurl:
Only use this method from the console; NEVER from remote. If you are using
telnet, xterm, or a dial-in, type ^C now or exit with no password.
Then run opiepasswd without the -c parameter.
Using MD5 to compute responses.
Enter new secret pass phrase:
Again new secret pass phrase:
ID unfurl OTP key is 499 to4268
MOS MALL GOAT ARM AVID COED
```

At the `Enter new secret pass phrase:` or `Enter secret password:` prompts, you should enter a password or phrase. Remember, this is not the password that you will use to login with, this is used to generate your one-time login keys. The "ID" line gives the parameters of your particular instance: your login name, the iteration count, and seed. When logging in the system will remember these parameters and present them back to you so you do not have to remember them. The last line gives the particular one-time password which corresponds to those parameters and your secret password; if you were to re-login immediately, this one-time password is the one you would use.

35.5.2. Insecure Connection Initialization

To initialize or change your secret password over an insecure connection, you will need to already have a secure connection to some place where you can run `opiekey`; this might be in the form of a shell prompt on a machine you trust. You will also need to make up an iteration count (100 is probably a good value), and you may make up your own seed or use a randomly-generated one. Over on the insecure connection (to the machine you are initializing), use `opiepasswd`:

```
% opiepasswd

Updating unfurl:
You need the response from an OTP generator.
Old secret pass phrase:
        otp-md5 498 to4268 ext
        Response: GAME GAG WELT OUT DOWN CHAT
New secret pass phrase:
        otp-md5 499 to4269
        Response: LINE PAP MILK NELL BUOY TROY

ID mark OTP key is 499 gr4269
LINE PAP MILK NELL BUOY TROY
```

To accept the default seed press `Return`. Then before entering an access password, move over to your secure connection and give it the same parameters:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

Now switch back over to the insecure connection, and copy the one-time password generated over to the relevant program.

35.5.3. Generating a Single One-time Password

Once you have initialized OPIE and login, you will be presented with a prompt like this:

```
% telnet example.com
Trying 10.0.0.1...
Connected to example.com
Escape character is '^]'.

FreeBSD/i386 (example.com) (ttypa)

login: <username>
otp-md5 498 gr4269 ext
```

```
Password:
```

As a side note, the OPIE prompts have a useful feature (not shown here): if you press `Return` at the password prompt, the prompter will turn echo on, so you can see what you are typing. This can be extremely useful if you are attempting to type in a password by hand, such as from a printout.

At this point you need to generate your one-time password to answer this login prompt. This must be done on a trusted system that you can run `opiekey` on. (There are versions of these for DOS, Windows® and Mac OS® as well.) They need the iteration count and the seed as command line options. You can cut-and-paste these right from the login prompt on the machine that you are logging in to.

On the trusted system:

```
% opiekey 498 to4268
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase:
GAME GAG WELT OUT DOWN CHAT
```

Now that you have your one-time password you can continue logging in.

35.5.4. Generating Multiple One-time Passwords

Sometimes you have to go places where you do not have access to a trusted machine or secure connection. In this case, it is possible to use the `opiekey` command to generate a number of one-time passwords beforehand to be printed out and taken with you. For example:

```
% opiekey -n 5 30 zz99999
Using the MD5 algorithm to compute response.
Reminder: Don't use opiekey from telnet or dial-in sessions.
Enter secret pass phrase: <secret password>
26: JOAN BORE FOSS DES NAY QUIT
27: LATE BIAS SLAY FOLK MUCH TRIG
28: SALT TIN ANTI LOON NEAL USE
29: RIO ODIN GO BYE FURY TIC
30: GREW JIVE SAN GIRD BOIL PHI
```

The `-n 5` requests five keys in sequence, the `30` specifies what the last iteration number should be. Note that these are printed out in *reverse* order of eventual use. If you are really paranoid, you might want to write the results down by hand; otherwise you can cut-and-paste into `lpr`. Note that each line shows both the iteration count and the one-time password; you may still find it handy to scratch off passwords as you use them.

35.5.5. Restricting Use of UNIX® Passwords

OPIE can restrict the use of UNIX® passwords based on the IP address of a login session. The

relevant file is /etc/opieaccess, which is present by default. Please check opieaccess(5) for more information on this file and which security considerations you should be aware of when using it.

Here is a sample opieaccess file:

```
permit 192.168.0.0 255.255.0.0
```

This line allows users whose IP source address (which is vulnerable to spoofing) matches the specified value and mask, to use UNIX® passwords at any time.

If no rules in opieaccess are matched, the default is to deny non-OPIE logins.

35.6. TCP Wrappers

Anyone familiar with inetd(8) has probably heard of TCP Wrappers at some point. But few individuals seem to fully comprehend its usefulness in a network environment. It seems that everyone wants to install a firewall to handle network connections. While a firewall has a wide variety of uses, there are some things that a firewall not handle such as sending text back to the connection originator. The TCP software does this and much more. In the next few sections many of the TCP Wrappers features will be discussed, and, when applicable, example configuration lines will be provided.

The TCP Wrappers software extends the abilities of `inetd` to provide support for every server daemon under its control. Using this method it is possible to provide logging support, return messages to connections, permit a daemon to only accept internal connections, etc. While some of these features can be provided by implementing a firewall, this will add not only an extra layer of protection but go beyond the amount of control a firewall can provide.

The added functionality of TCP Wrappers should not be considered a replacement for a good firewall. TCP Wrappers can be used in conjunction with a firewall or other security enhancements though and it can serve nicely as an extra layer of protection for the system.

Since this is an extension to the configuration of `inetd`, the reader is expected have read the inetd configuration section.

While programs run by inetd(8) are not exactly "daemons", they have traditionally been called daemons. This is the term we will use in this section too.

35.6.1. Initial Configuration

The only requirement of using TCP Wrappers in FreeBSD is to ensure the `inetd` server is started from rc.conf with the `-Ww` option; this is the default setting. Of course, proper configuration of /etc/hosts.allow is also expected, but syslogd(8) will throw messages in the system logs in these cases.

Unlike other implementations of TCP Wrappers, the use of hosts.deny has been deprecated. All configuration options should be placed in /etc/hosts.allow.

In the simplest configuration, daemon connection policies are set to either be permitted or blocked depending on the options in /etc/hosts.allow. The default configuration in FreeBSD is to allow a connection to every daemon started with `inetd`. Changing this will be discussed only after the basic configuration is covered.

Basic configuration usually takes the form of `daemon : address : action`. Where `daemon` is the daemon name which `inetd` started. The `address` can be a valid hostname, an IP address or an IPv6 address enclosed in brackets ([ ]). The action field can be either allow or deny to grant or deny access appropriately. Keep in mind that configuration works off a first rule match semantic, meaning that the configuration file is scanned in ascending order for a matching rule. When a match is found the rule is applied and the search process will halt.

Several other options exist but they will be explained in a later section. A simple configuration line may easily be constructed from that information alone. For example, to allow POP3 connections via the mail/qpopper daemon, the following lines should be appended to hosts.allow:

```
# This line is required for POP3 connections:
qpopper : ALL : allow
```

After adding this line, `inetd` will need restarted. This can be accomplished by use of the kill(1) command, or with the restart parameter with /etc/rc.d/inetd.

35.6.2. Advanced Configuration

TCP Wrappers has advanced options too; they will allow for more control over the way connections are handled. In some cases it may be a good idea to return a comment to certain hosts or daemon connections. In other cases, perhaps a log file should be recorded or an email sent to the administrator. Other situations may require the use of a service for local connections only. This is all possible through the use of configuration options known as `wildcards`, expansion characters and external command execution. The next two sections are written to cover these situations.

35.6.2.1. External Commands

Suppose that a situation occurs where a connection should be denied yet a reason should be sent to the individual who attempted to establish that connection. How could it be done? That action can be made possible by using the `twist` option. When a connection attempt is made, `twist` will be called to execute a shell command or script. An example already exists in the hosts.allow file:

```
# The rest of the daemons are protected.
ALL : ALL \
        : severity auth.info \
        : twist /bin/echo "You are not welcome to use %d from %h."
```

This example shows that the message, "You are not allowed to use `daemon` from `hostname`." will be returned for any daemon not previously configured in the access file. This is extremely useful for sending a reply back to the connection initiator right after the established connection is dropped. Note that any message returned *must* be wrapped in quote `"` characters; there are no exceptions to

this rule.

It may be possible to launch a denial of service attack on the server if an attacker, or group of attackers could flood these daemons with connection requests.

Another possibility is to use the `spawn` option in these cases. Like `twist`, the `spawn` implicitly denies the connection and may be used to run external shell commands or scripts. Unlike `twist`, `spawn` will not send a reply back to the individual who established the connection. For an example, consider the following configuration line:

```
# We do not allow connections from example.com:
ALL : .example.com \
    : spawn (/bin/echo %a from %h attempted to access %d >> \
      /var/log/connections.log) \
    : deny
```

This will deny all connection attempts from the `*.example.com` domain; simultaneously logging the hostname, IP address and the daemon which they attempted to access in the /var/log/connections.log file.

Aside from the already explained substitution characters above, e.g. %a, a few others exist. See the hosts_access(5) manual page for the complete list.

35.6.2.2. Wildcard Options

Thus far the `ALL` example has been used continuously throughout the examples. Other options exist which could extend the functionality a bit further. For instance, `ALL` may be used to match every instance of either a daemon, domain or an IP address. Another wildcard available is `PARANOID` which may be used to match any host which provides an IP address that may be forged. In other words, `paranoid` may be used to define an action to be taken whenever a connection is made from an IP address that differs from its hostname. The following example may shed some more light on this discussion:

```
# Block possibly spoofed requests to sendmail:
sendmail : PARANOID : deny
```

In that example all connection requests to `sendmail` which have an IP address that varies from its hostname will be denied.

Using the `PARANOID` may severely cripple servers if the client or server has a broken DNS setup. Administrator discretion is advised.

To learn more about wildcards and their associated functionality, see the hosts_access(5) manual page.

Before any of the specific configuration lines above will work, the first configuration line should be commented out in hosts.allow. This was noted at the beginning of this section.

35.7. KerberosIV

Kerberos is a network add-on system/protocol that allows users to authenticate themselves through the services of a secure server. Services such as remote login, remote copy, secure inter-system file copying and other high-risk tasks are made considerably safer and more controllable.

The following instructions can be used as a guide on how to set up Kerberos as distributed for FreeBSD. However, you should refer to the relevant manual pages for a complete description.

35.7.1. Installing KerberosIV

Kerberos is an optional component of FreeBSD. The easiest way to install this software is by selecting the `krb4` or `krb5` distribution in sysinstall during the initial installation of FreeBSD. This will install the "eBones" (KerberosIV) or "Heimdal" (Kerberos5) implementation of Kerberos. These implementations are included because they are developed outside the USA/Canada and were thus available to system owners outside those countries during the era of restrictive export controls on cryptographic code from the USA.

Alternatively, the MIT implementation of Kerberos is available from the Ports Collection as security/krb5.

35.7.2. Creating the Initial Database

This is done on the Kerberos server only. First make sure that you do not have any old Kerberos databases around. You should change to the directory /etc/kerberosIV and check that only the following files are present:

```
d /etc/kerberosIV
# ls
README      krb.conf        krb.realms
```

If any additional files (such as principal.* or master_key) exist, then use the `kdb_destroy` command to destroy the old Kerberos database, or if Kerberos is not running, simply delete the extra files.

You should now edit the krb.conf and krb.realms files to define your Kerberos realm. In this case the realm will be `EXAMPLE.COM` and the server is `grunt.example.com`. We edit or create the krb.conf file:

```
# cat krb.conf
EXAMPLE.COM
EXAMPLE.COM grunt.example.com admin server
CS.BERKELEY.EDU okeeffe.berkeley.edu
ATHENA.MIT.EDU kerberos.mit.edu
ATHENA.MIT.EDU kerberos-1.mit.edu
ATHENA.MIT.EDU kerberos-2.mit.edu
ATHENA.MIT.EDU kerberos-3.mit.edu
LCS.MIT.EDU kerberos.lcs.mit.edu
TELECOM.MIT.EDU bitsy.mit.edu
```

```
ARC.NASA.GOV trident.arc.nasa.gov
```

In this case, the other realms do not need to be there. They are here as an example of how a machine may be made aware of multiple realms. You may wish to not include them for simplicity.

The first line names the realm in which this system works. The other lines contain realm/host entries. The first item on a line is a realm, and the second is a host in that realm that is acting as a "key distribution center". The words `admin server` following a host's name means that host also provides an administrative database server. For further explanation of these terms, please consult the Kerberos manual pages.

Now we have to add `grunt.example.com` to the `EXAMPLE.COM` realm and also add an entry to put all hosts in the `.example.com` domain in the `EXAMPLE.COM` realm. The krb.realms file would be updated as follows:

```
# cat krb.realms
grunt.example.com EXAMPLE.COM
.example.com EXAMPLE.COM
.berkeley.edu CS.BERKELEY.EDU
.MIT.EDU ATHENA.MIT.EDU
.mit.edu ATHENA.MIT.EDU
```

Again, the other realms do not need to be there. They are here as an example of how a machine may be made aware of multiple realms. You may wish to remove them to simplify things.

The first line puts the *specific* system into the named realm. The rest of the lines show how to default systems of a particular subdomain to a named realm.

Now we are ready to create the database. This only needs to run on the Kerberos server (or Key Distribution Center). Issue the `kdb_init` command to do this:

```
# kdb_init
Realm name [default  ATHENA.MIT.EDU ]: EXAMPLE.COM
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.

Enter Kerberos master key:
```

Now we have to save the key so that servers on the local machine can pick it up. Use the `kstash` command to do this:

```
# kstash

Enter Kerberos master key:

Current Kerberos master key version is 1.
```

```
Master key entered. BEWARE!
```

This saves the encrypted master password in /etc/kerberosIV/master_key.

35.7.3. Making It All Run

Two principals need to be added to the database for *each* system that will be secured with Kerberos. Their names are `kpasswd` and `rcmd`. These two principals are made for each system, with the instance being the name of the individual system.

These daemons, kpasswd and rcmd allow other systems to change Kerberos passwords and run commands like rcp(1), rlogin(1) and rsh(1).

Now let us add these entries:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: passwd
Instance: grunt

<Not found>, Create [y] ? y

Principal: passwd, Instance: grunt, kdc_key_ver: 1
New Password:                    <---- enter RANDOM here
Verifying password

New Password: <---- enter RANDOM here

Random password [y] ? y

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name: rcmd
Instance: grunt

<Not found>, Create [y] ?

Principal: rcmd, Instance: grunt, kdc_key_ver: 1
```

```
New Password:       <---- enter RANDOM here
Verifying password

New Password:           <---- enter RANDOM here

Random password [y] ?

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:         <---- null entry here will cause an exit
```

35.7.4. Creating the Server File

We now have to extract all the instances which define the services on each machine. For this we use the `ext_srvtab` command. This will create a file which must be copied or moved *by secure means* to each Kerberos client's /etc directory. This file must be present on each server and client, and is crucial to the operation of Kerberos.

```
# ext_srvtab grunt
Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered. BEWARE!
Generating 'grunt-new-srvtab'....
```

Now, this command only generates a temporary file which must be renamed to srvtab so that all the servers can pick it up. Use the mv(1) command to move it into place on the original system:

```
# mv grunt-new-srvtab srvtab
```

If the file is for a client system, and the network is not deemed safe, then copy the client-new-srvtab to removable media and transport it by secure physical means. Be sure to rename it to srvtab in the client's /etc directory, and make sure it is mode 600:

```
# mv grumble-new-srvtab srvtab
# chmod 600 srvtab
```

35.7.5. Populating the Database

We now have to add some user entries into the database. First let us create an entry for the user `jane`. Use the `kdb_edit` command to do this:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance:

<Not found>, Create [y] ? y

Principal: jane, Instance: , kdc_key_ver: 1
New Password:                <---- enter a secure password here
Verifying password

New Password:                <---- re-enter the password here
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ?
Attributes [ 0 ] ?
Edit O.K.
Principal name:        <---- null entry here will cause an exit
```

35.7.6. Testing It All Out

First we have to start the Kerberos daemons. Note that if you have correctly edited your /etc/rc.conf then this will happen automatically when you reboot. This is only necessary on the Kerberos server. Kerberos clients will automatically get what they need from the /etc/kerberosIV directory.

```
# kerberos &
Kerberos server starting
Sleep forever on error
Log file is /var/log/kerberos.log
Current Kerberos master key version is 1.

Master key entered. BEWARE!

Current Kerberos master key version is 1
Local realm: EXAMPLE.COM
# kadmind -n &
KADM Server KADM0.0A initializing
Please do not use 'kill -9' to kill this job, use a
regular kill instead
```

```
Current Kerberos master key version is 1.

Master key entered.  BEWARE!
```

Now we can try using the `kinit` command to get a ticket for the ID `jane` that we created above:

```
% kinit jane
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane"
Password:
```

Try listing the tokens using `klist` to see if we really have them:

```
% klist
Ticket file:    /tmp/tkt245
Principal:      jane@EXAMPLE.COM

  Issued           Expires          Principal
Apr 30 11:23:22  Apr 30 19:23:22  krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

Now try changing the password using passwd(1) to check if the kpasswd daemon can get authorization to the Kerberos database:

```
% passwd
realm EXAMPLE.COM
Old password for jane:
New Password for jane:
Verifying password
New Password for jane:
Password changed.
```

35.7.7. Adding `su` Privileges

Kerberos allows us to give *each* user who needs `root` privileges their own *separate* su(1) password. We could now add an ID which is authorized to su(1) to `root`. This is controlled by having an instance of `root` associated with a principal. Using `kdb_edit` we can create the entry `jane.root` in the Kerberos database:

```
# kdb_edit
Opening database...

Enter Kerberos master key:

Current Kerberos master key version is 1.

Master key entered.  BEWARE!
```

```
Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: jane
Instance: root

<Not found>, Create [y] ? y

Principal: jane, Instance: root, kdc_key_ver: 1
New Password:                    <---- enter a SECURE password here
Verifying password

New Password:            <---- re-enter the password here

Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 2000-01-01 ] ?
Max ticket lifetime (*5 minutes) [ 255 ] ? 12 <--- Keep this short!
Attributes [ 0 ] ?
Edit O.K.
Principal name:              <---- null entry here will cause an exit
```

Now try getting tokens for it to make sure it works:

```
# kinit jane.root
MIT Project Athena (grunt.example.com)
Kerberos Initialization for "jane.root"
Password:
```

Now we need to add the user to `root`'s .klogin file:

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

Now try doing the su(1):

```
% su
Password:
```

and take a look at what tokens we have:

```
# klist
Ticket file:    /tmp/tkt_root_245
Principal:      jane.root@EXAMPLE.COM

  Issued           Expires          Principal
```

```
May  2 20:43:12  May  3 04:43:12  krbtgt.EXAMPLE.COM@EXAMPLE.COM
```

35.7.8. Using Other Commands

In an earlier example, we created a principal called `jane` with an instance `root`. This was based on a user with the same name as the principal, and this is a Kerberos default; that a `<principal>.<instance>` of the form `<username>. root` will allow that `<username>` to su(1) to `root` if the necessary entries are in the .klogin file in `root`'s home directory:

```
# cat /root/.klogin
jane.root@EXAMPLE.COM
```

Likewise, if a user has in their own home directory lines of the form:

```
% cat ~/.klogin
jane@EXAMPLE.COM
jack@EXAMPLE.COM
```

This allows anyone in the `EXAMPLE.COM` realm who has authenticated themselves as `jane` or `jack` (via `kinit`, see above) to access to `jane`'s account or files on this system (`grunt`) via rlogin(1), rsh(1) or rcp(1).

For example, `jane` now logs into another system using Kerberos:

```
% kinit
MIT Project Athena (grunt.example.com)
Password:
% rlogin grunt
Last login: Mon May  1 21:14:47 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.   All rights reserved.

FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

Or `jack` logs into `jane`'s account on the same machine (`jane` having set up the .klogin file as above, and the person in charge of Kerberos having set up principal *jack* with a null instance):

```
% kinit
% rlogin grunt -l jane
MIT Project Athena (grunt.example.com)
Password:
Last login: Mon May  1 21:16:55 from grumble
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.   All rights reserved.
FreeBSD BUILT-19950429 (GR386) #0: Sat Apr 29 17:50:09 SAT 1995
```

35.8. Kerberos5

Every FreeBSD release beyond FreeBSD-5.1 includes support only for Kerberos5. Hence Kerberos5 is the only version included, and its configuration is similar in many aspects to that of KerberosIV. The following information only applies to Kerberos5 in post FreeBSD-5.0 releases. Users who wish to use the KerberosIV package may install the security/krb4 port.

Kerberos is a network add-on system/protocol that allows users to authenticate themselves through the services of a secure server. Services such as remote login, remote copy, secure inter-system file copying and other high-risk tasks are made considerably safer and more controllable.

Kerberos can be described as an identity-verifying proxy system. It can also be described as a trusted third-party authentication system. Kerberos provides only one function - the secure authentication of users on the network. It does not provide authorization functions (what users are allowed to do) or auditing functions (what those users did). After a client and server have used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.

Therefore it is highly recommended that Kerberos be used with other security methods which provide authorization and audit services.

The following instructions can be used as a guide on how to set up Kerberos as distributed for FreeBSD. However, you should refer to the relevant manual pages for a complete description.

For purposes of demonstrating a Kerberos installation, the various name spaces will be handled as follows:

- The DNS domain ("zone") will be example.org.
- The Kerberos realm will be EXAMPLE.ORG.

Please use real domain names when setting up Kerberos even if you intend to run it internally. This avoids DNS problems and assures inter-operation with other Kerberos realms.

35.8.1. History

Kerberos was created by MIT as a solution to network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection.

Kerberos is both the name of a network authentication protocol and an adjective to describe programs that implement the program (Kerberos telnet, for example). The current version of the protocol is version 5, described in RFC 1510.

Several free implementations of this protocol are available, covering a wide range of operating systems. The Massachusetts Institute of Technology (MIT), where Kerberos was originally developed, continues to develop their Kerberos package. It is commonly used in the US as a cryptography product, as such it has historically been affected by US export regulations. The MITKerberos is available as a port (security/krb5). Heimdal Kerberos is another version 5

implementation, and was explicitly developed outside of the US to avoid export regulations (and is thus often included in non-commercial UNIX® variants). The Heimdal Kerberos distribution is available as a port (security/heimdal), and a minimal installation of it is included in the base FreeBSD install.

In order to reach the widest audience, these instructions assume the use of the Heimdal distribution included in FreeBSD.

35.8.2. Setting up a Heimdal KDC

The Key Distribution Center (KDC) is the centralized authentication service that Kerberos provides - it is the computer that issues Kerberos tickets. The KDC is considered "trusted" by all other computers in the Kerberos realm, and thus has heightened security concerns.

Note that while running the Kerberos server requires very few computing resources, a dedicated machine acting only as a KDC is recommended for security reasons.

To begin setting up a KDC, ensure that your /etc/rc.conf file contains the correct settings to act as a KDC (you may need to adjust paths to reflect your own system):

```
kerberos5_server_enable="YES"
kadmind5_server_enable="YES"
```

Next we will set up your Kerberos config file, /etc/krb5.conf:

```
[libdefaults]
    default_realm = EXAMPLE.ORG
[realms]
    EXAMPLE.ORG = {
        kdc = kerberos.example.org
        admin_server = kerberos.example.org
    }
[domain_realm]
    .example.org = EXAMPLE.ORG
```

Note that this /etc/krb5.conf file implies that your KDC will have the fully-qualified hostname of `kerberos.example.org`. You will need to add a CNAME (alias) entry to your zone file to accomplish this if your KDC has a different hostname.

For large networks with a properly configured BINDDNS server, the above example could be trimmed to:

```
[libdefaults]
      default_realm = EXAMPLE.ORG
```

With the following lines being appended to the `example.org` zonefile:

```
_kerberos._udp      IN  SRV     01 00 88 kerberos.example.org.
_kerberos._tcp      IN  SRV     01 00 88 kerberos.example.org.
_kpasswd._udp       IN  SRV     01 00 464 kerberos.example.org.
_kerberos-adm._tcp  IN  SRV     01 00 749 kerberos.example.org.
_kerberos           IN  TXT     EXAMPLE.ORG
```

For clients to be able to find the Kerberos services, you *must* have either a fully configured /etc/krb5.conf or a minimally configured /etc/krb5.conf*and* a properly configured DNS server.

Next we will create the Kerberos database. This database contains the keys of all principals encrypted with a master password. You are not required to remember this password, it will be stored in a file (/var/heimdal/m-key). To create the master key, run `kstash` and enter a password.

Once the master key has been created, you can initialize the database using the `kadmin` program with the `-l` option (standing for "local"). This option instructs `kadmin` to modify the database files directly rather than going through the `kadmind` network service. This handles the chicken-and-egg problem of trying to connect to the database before it is created. Once you have the `kadmin` prompt, use the `init` command to create your realms initial database.

Lastly, while still in `kadmin`, create your first principal using the `add` command. Stick to the defaults options for the principal for now, you can always change them later with the `modify` command. Note that you can use the `?` command at any prompt to see the available options.

A sample database creation session is shown below:

```
# kstash
Master key: xxxxxxxx
Verifying password - Master key: xxxxxxxx

# kadmin -l
kadmin> init EXAMPLE.ORG
Realm max ticket life [unlimited]:
kadmin> add tillman
Max ticket life [unlimited]:
Max renewable life [unlimited]:
Attributes []:
Password: xxxxxxxx
Verifying password - Password: xxxxxxxx
```

Now it is time to start up the KDC services. Run `/etc/rc.d/kerberos start` and `/etc/rc.d/kadmind start` to bring up the services. Note that you will not have any kerberized daemons running at this point but you should be able to confirm the that the KDC is functioning by obtaining and listing a ticket for the principal (user) that you just created from the command-line of the KDC itself:

```
% kinit tillman
tillman@EXAMPLE.ORG's Password:
```

```
% klist
Credentials cache: FILE:/tmp/krb5cc_500
    Principal: tillman@EXAMPLE.ORG

  Issued           Expires          Principal
Aug 27 15:37:58  Aug 28 01:37:58  krbtgt/EXAMPLE.ORG@EXAMPLE.ORG
```

The ticket can then be revoked when you have finished:

```
% k5destroy
```

35.8.3. Kerberos enabling a server with Heimdal services

First, we need a copy of the Kerberos configuration file, /etc/krb5.conf. To do so, simply copy it over to the client computer from the KDC in a secure fashion (using network utilities, such as scp(1), or physically via a floppy disk).

Next you need a /etc/krb5.keytab file. This is the major difference between a server providing Kerberos enabled daemons and a workstation - the server must have a keytab file. This file contains the server's host key, which allows it and the KDC to verify each others identity. It must be transmitted to the server in a secure fashion, as the security of the server can be broken if the key is made public. This explicitly means that transferring it via a clear text channel, such as FTP, is a very bad idea.

Typically, you transfer to the keytab to the server using the `kadmin` program. This is handy because you also need to create the host principal (the KDC end of the krb5.keytab) using `kadmin`.

Note that you must have already obtained a ticket and that this ticket must be allowed to use the `kadmin` interface in the kadmind.acl. See the section titled "Remote administration" in the Heimdal info pages (`info heimdal`) for details on designing access control lists. If you do not want to enable remote `kadmin` access, you can simply securely connect to the KDC (via local console, ssh(1) or Kerberos telnet(1)) and perform administration locally using `kadmin -l`.

After installing the /etc/krb5.conf file, you can use `kadmin` from the Kerberos server. The `add --random-key` command will let you add the server's host principal, and the `ext` command will allow you to extract the server's host principal to its own keytab. For example:

```
# kadmin
kadmin> add --random-key host/myserver.example.org
Max ticket life [unlimited]:
Max renewable life [unlimited]:
Attributes []:
kadmin> ext host/myserver.example.org
kadmin> exit
```

Note that the `ext` command (short for "extract") stores the extracted key in /etc/krb5.keytab by

default.

If you do not have `kadmind` running on the KDC (possibly for security reasons) and thus do not have access to `kadmin` remotely, you can add the host principal (`host/myserver.EXAMPLE.ORG`) directly on the KDC and then extract it to a temporary file (to avoid over-writing the /etc/krb5.keytab on the KDC) using something like this:

```
# kadmin
kadmin> ext --keytab=/tmp/example.keytab host/myserver.example.org
kadmin> exit
```

You can then securely copy the keytab to the server computer (using `scp` or a floppy, for example). Be sure to specify a non-default keytab name to avoid over-writing the keytab on the KDC.

At this point your server can communicate with the KDC (due to its krb5.conf file) and it can prove its own identity (due to the krb5.keytab file). It is now ready for you to enable some Kerberos services. For this example we will enable the `telnet` service by putting a line like this into your /etc/inetd.conf and then restarting the inetd(8) service with `/etc/rc.d/inetd restart`:

```
telnet    stream  tcp     nowait  root    /usr/libexec/telnetd  telnetd -a user
```

The critical bit is that the `-a` (for authentication) type is set to user. Consult the telnetd(8) manual page for more details.

35.8.4. Kerberos enabling a client with Heimdal

Setting up a client computer is almost trivially easy. As far as Kerberos configuration goes, you only need the Kerberos configuration file, located at /etc/krb5.conf. Simply securely copy it over to the client computer from the KDC.

Test your client computer by attempting to use `kinit`, `klist`, and `kdestroy` from the client to obtain, show, and then delete a ticket for the principal you created above. You should also be able to use Kerberos applications to connect to Kerberos enabled servers, though if that does not work and obtaining a ticket does the problem is likely with the server and not with the client or the KDC.

When testing an application like `telnet`, try using a packet sniffer (such as tcpdump(1)) to confirm that your password is not sent in the clear. Try using `telnet` with the `-x` option, which encrypts the entire data stream (similar to `ssh`).

Various non-core Kerberos client applications are also installed by default. This is where the "minimal" nature of the base Heimdal installation is felt: `telnet` is the only Kerberos enabled service.

The Heimdal port adds some of the missing client applications: Kerberos enabled versions of `ftp`, `rsh`, `rcp`, `rlogin`, and a few other less common programs. The MIT port also contains a full suite of Kerberos client applications.

35.8.5. User configuration files: .k5login and .k5users

Users within a realm typically have their Kerberos principal (such as `tillman@EXAMPLE.ORG`) mapped to a local user account (such as a local account named `tillman`). Client applications such as `telnet` usually do not require a user name or a principal.

Occasionally, however, you want to grant access to a local user account to someone who does not have a matching Kerberos principal. For example, `tillman@EXAMPLE.ORG` may need access to the local user account `webdevelopers`. Other principals may also need access to that local account.

The .k5login and .k5users files, placed in a users home directory, can be used similar to a powerful combination of .hosts and .rhosts, solving this problem. For example, if a .k5login with the following contents:

```
tillman@example.org
jdoe@example.org
```

Were to be placed into the home directory of the local user `webdevelopers` then both principals listed would have access to that account without requiring a shared password.

Reading the manual pages for these commands is recommended. Note that the `ksu` manual page covers .k5users.

35.8.6. Kerberos Tips, Tricks, and Troubleshooting

- When using either the Heimdal or MITKerberos ports ensure that your `PATH` environment variable lists the Kerberos versions of the client applications before the system versions.
- Do all the computers in your realm have synchronized time settings? If not, authentication may fail. Συγχρονισμός Ρολογιού Συστήματος με NTP describes how to synchronize clocks using NTP.
- MIT and Heimdal inter-operate nicely. Except for `kadmin`, the protocol for which is not standardized.
- If you change your hostname, you also need to change your `host/` principal and update your keytab. This also applies to special keytab entries like the `www/` principal used for Apache's www/mod_auth_kerb.
- All hosts in your realm must be resolvable (both forwards and reverse) in DNS (or /etc/hosts as a minimum). CNAMEs will work, but the A and PTR records must be correct and in place. The error message is not very intuitive: `Kerberos5 refuses authentication because Read req failed: Key table entry not found`.
- Some operating systems that may being acting as clients to your KDC do not set the permissions for `ksu` to be setuid `root`. This means that `ksu` does not work, which is a good security idea but annoying. This is not a KDC error.
- With MITKerberos, if you want to allow a principal to have a ticket life longer than the default ten hours, you must use `modify_principal` in `kadmin` to change the maxlife of both the principal in question and the `krbtgt` principal. Then the principal can use the `-l` option with `kinit` to request a ticket with a longer lifetime.

If you run a packet sniffer on your KDC to add in troubleshooting and then run `kinit` from a workstation, you will notice that your TGT is sent immediately upon running `kinit` - even before you type your password! The explanation is that the Kerberos server freely transmits a TGT (Ticket Granting Ticket) to any unauthorized request; however, every TGT is encrypted in a key derived from the user's password. Therefore, when a user types their password it is not being sent to the KDC, it is being used to decrypt the TGT that `kinit` already obtained. If the decryption process results in a valid ticket with a valid time stamp, the user has valid Kerberos credentials. These credentials include a session key for establishing secure communications with the Kerberos server in the future, as well as the actual ticket-granting ticket, which is actually encrypted with the Kerberos server's own key. This second layer of encryption is unknown to the user, but it is what allows the Kerberos server to verify the authenticity of each TGT.

- If you want to use long ticket lifetimes (a week, for example) and you are using OpenSSH to connect to the machine where your ticket is stored, make sure that Kerberos `TicketCleanup` is set to `no` in your sshd_config or else your tickets will be deleted when you log out.
- Remember that host principals can have a longer ticket lifetime as well. If your user principal has a lifetime of a week but the host you are connecting to has a lifetime of nine hours, you will have an expired host principal in your cache and the ticket cache will not work as expected.
- When setting up a krb5.dict file to prevent specific bad passwords from being used (the manual page for `kadmind` covers this briefly), remember that it only applies to principals that have a password policy assigned to them. The krb5.dict files format is simple: one string per line. Creating a symbolic link to /usr/shared/dict/words might be useful.

35.8.7. Differences with the MIT port

The major difference between the MIT and Heimdal installs relates to the `kadmin` program which has a different (but equivalent) set of commands and uses a different protocol. This has a large implications if your KDC is MIT as you will not be able to use the Heimdal `kadmin` program to administer your KDC remotely (or vice versa, for that matter).

The client applications may also take slightly different command line options to accomplish the same tasks. Following the instructions on the MITKerberos web site (http://web.mit.edu/Kerberos/www/) is recommended. Be careful of path issues: the MIT port installs into /usr/local/ by default, and the "normal" system applications may be run instead of MIT if your `PATH` environment variable lists the system directories first.

With the MITsecurity/krb5 port that is provided by FreeBSD, be sure to read the /usr/local/shared/doc/krb5/README.FreeBSD file installed by the port if you want to understand why logins via `telnetd` and `klogind` behave somewhat oddly. Most importantly, correcting the "incorrect permissions on cache file" behavior requires that the `login.krb5` binary be used for authentication so that it can properly change ownership for the forwarded credentials.

The rc.conf must also be modified to contain the following configuration:

```
kerberos5_server="/usr/local/sbin/krb5kdc"
kadmind5_server="/usr/local/sbin/kadmind"
kerberos5_server_enable="YES"
kadmind5_server_enable="YES"
```

This is done because the applications for MIT kerberos installs binaries in the /usr/local hierarchy.

35.8.8. Mitigating limitations found in Kerberos

35.8.8.1. Kerberos is an all-or-nothing approach

Every service enabled on the network must be modified to work with Kerberos (or be otherwise secured against network attacks) or else the users credentials could be stolen and re-used. An example of this would be Kerberos enabling all remote shells (via `rsh` and `telnet`, for example) but not converting the POP3 mail server which sends passwords in plain text.

35.8.8.2. Kerberos is intended for single-user workstations

In a multi-user environment, Kerberos is less secure. This is because it stores the tickets in the /tmp directory, which is readable by all users. If a user is sharing a computer with several other people simultaneously (i.e. multi-user), it is possible that the user's tickets can be stolen (copied) by another user.

This can be overcome with the `-c` filename command-line option or (preferably) the `KRB5CCNAME` environment variable, but this is rarely done. In principal, storing the ticket in the users home directory and using simple file permissions can mitigate this problem.

35.8.8.3. The KDC is a single point of failure

By design, the KDC must be as secure as the master password database is contained on it. The KDC should have absolutely no other services running on it and should be physically secured. The danger is high because Kerberos stores all passwords encrypted with the same key (the "master" key), which in turn is stored as a file on the KDC.

As a side note, a compromised master key is not quite as bad as one might normally fear. The master key is only used to encrypt the Kerberos database and as a seed for the random number generator. As long as access to your KDC is secure, an attacker cannot do much with the master key.

Additionally, if the KDC is unavailable (perhaps due to a denial of service attack or network problems) the network services are unusable as authentication can not be performed, a recipe for a denial-of-service attack. This can alleviated with multiple KDCs (a single master and one or more slaves) and with careful implementation of secondary or fall-back authentication (PAM is excellent for this).

35.8.8.4. Kerberos Shortcomings

Kerberos allows users, hosts and services to authenticate between themselves. It does not have a mechanism to authenticate the KDC to the users, hosts or services. This means that a trojanned `kinit` (for example) could record all user names and passwords. Something like security/tripwire or

other file system integrity checking tools can alleviate this.

35.8.9. Resources and further information

- The Kerberos FAQ
- Designing an Authentication System: a Dialog in Four Scenes
- RFC 1510, The Kerberos Network Authentication Service (V5)
- MIT Kerberos home page
- Heimdal Kerberos home page

35.9. OpenSSL

One feature that many users overlook is the OpenSSL toolkit included in FreeBSD. OpenSSL provides an encryption transport layer on top of the normal communications layer; thus allowing it to be intertwined with many network applications and services.

Some uses of OpenSSL may include encrypted authentication of mail clients, web based transactions such as credit card payments and more. Many ports such as www/apache13-ssl, and mail/sylpheed-claws will offer compilation support for building with OpenSSL.

In most cases the Ports Collection will attempt to build the security/openssl port unless the `WITH_OPENSSL_BASE` make variable is explicitly set to "yes".

The version of OpenSSL included in FreeBSD supports Secure Sockets Layer v2/v3 (SSLv2/SSLv3), Transport Layer Security v1 (TLSv1) network security protocols and can be used as a general cryptographic library.

While OpenSSL supports the IDEA algorithm, it is disabled by default due to United States patents. To use it, the license should be reviewed and, if the restrictions are acceptable, the `MAKE_IDEA` variable must be set in make.conf.

One of the most common uses of OpenSSL is to provide certificates for use with software applications. These certificates ensure that the credentials of the company or individual are valid and not fraudulent. If the certificate in question has not been verified by one of the several "Certificate Authorities", or CAs, a warning is usually produced. A Certificate Authority is a company, such as VeriSign, which will sign certificates in order to validate credentials of individuals or companies. This process has a cost associated with it and is definitely not a requirement for using certificates; however, it can put some of the more paranoid users at ease.

35.9.1. Generating Certificates

To generate a certificate, the following command is available:

```
# openssl req -new -nodes -out req.pem -keyout cert.pem
Generating a 1024 bit RSA private key
..............++++++
```

```
.....................................++++++
writing new private key to 'cert.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PA
Locality Name (eg, city) []:Pittsburgh
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:Systems Administrator
Common Name (eg, YOUR name) []:localhost.example.org
Email Address []:trhodes@FreeBSD.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:SOME PASSWORD
An optional company name []:Another Name
```

Notice the response directly after the "Common Name" prompt shows a domain name. This prompt requires a server name to be entered for verification purposes; placing anything but a domain name would yield a useless certificate. Other options, for instance expire time, alternate encryption algorithms, etc. are available. A complete list may be obtained by viewing the openssl(1) manual page.

Two files should now exist in the directory in which the aforementioned command was issued. The certificate request, req.pem, may be sent to a certificate authority who will validate the credentials that you entered, sign the request and return the certificate to you. The second file created will be named cert.pem and is the private key for the certificate and should be protected at all costs; if this falls in the hands of others it can be used to impersonate you (or your server).

In cases where a signature from a CA is not required, a self signed certificate can be created. First, generate the RSA key:

```
# openssl dsaparam -rand -genkey -out myRSA.key 1024
```

Next, generate the CA key:

```
# openssl gendsa -des3 -out myca.key myRSA.key
```

Use this key to create the certificate:

```
# openssl req -new -x509 -days 365 -key myca.key -out new.crt
```

Two new files should appear in the directory: a certificate authority signature file, myca.key and the certificate itself, new.crt. These should be placed in a directory, preferably under /etc, which is readable only by `root`. Permissions of 0700 should be fine for this and they can be set with the `chmod` utility.

35.9.2. Using Certificates, an Example

So what can these files do? A good use would be to encrypt connections to the SendmailMTA. This would dissolve the use of clear text authentication for users who send mail via the local MTA.

This is not the best use in the world as some MUAs will present the user with an error if they have not installed the certificate locally. Refer to the documentation included with the software for more information on certificate installation.

The following lines should be placed inside the local .mc file:

```
dnl SSL Options
define(`confCACERT_PATH',`/etc/certs')dnl
define(`confCACERT',`/etc/certs/new.crt')dnl
define(`confSERVER_CERT',`/etc/certs/new.crt')dnl
define(`confSERVER_KEY',`/etc/certs/myca.key')dnl
define(`confTLS_SRV_OPTIONS', `V')dnl
```

Where /etc/certs/ is the directory to be used for storing the certificate and key files locally. The last few requirements are a rebuild of the local .cf file. This is easily achieved by typing `make`install within the /etc/mail directory. Follow that up with `make`restart which should start the Sendmail daemon.

If all went well there will be no error messages in the /var/log/maillog file and Sendmail will show up in the process list.

For a simple test, simply connect to the mail server using the telnet(1) utility:

```
# telnet example.com 25
Trying 192.0.34.166...
Connected to example.com.
Escape character is '^]'.
220 example.com ESMTP Sendmail 8.12.10/8.12.10; Tue, 31 Aug 2004 03:41:22 -0400 (EDT)
ehlo example.com
250-example.com Hello example.com [192.0.34.166], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE
250-DSN
```

```
250-ETRN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
quit
221 2.0.0 example.com closing connection
Connection closed by foreign host.
```

If the "STARTTLS" line appears in the output then everything is working correctly.

35.10. VPN over IPsec

Creating a VPN between two networks, separated by the Internet, using FreeBSD gateways.

35.10.1. Understanding IPsec

This section will guide you through the process of setting up IPsec, and to use it in an environment which consists of FreeBSD and Microsoft® Windows® 2000/XP machines, to make them communicate securely. In order to set up IPsec, it is necessary that you are familiar with the concepts of building a custom kernel (see Ρυθμίζοντας τον Πυρήνα του FreeBSD).

IPsec is a protocol which sits on top of the Internet Protocol (IP) layer. It allows two or more hosts to communicate in a secure manner (hence the name). The FreeBSD IPsec "network stack" is based on the KAME implementation, which has support for both protocol families, IPv4 and IPv6.

FreeBSD contains a "hardware accelerated" IPsec stack, known as "Fast IPsec", that was obtained from OpenBSD. It employs cryptographic hardware (whenever possible) via the crypto(4) subsystem to optimize the performance of IPsec. This subsystem is new, and does not support all the features that are available in the KAME version of IPsec. However, in order to enable hardware-accelerated IPsec, the following kernel option has to be added to your kernel configuration file:

```
options   FAST_IPSEC  # new IPsec (cannot define w/ IPSEC)
```

Note, that it is not currently possible to use the "Fast IPsec" subsystem in lieu of the KAME implementation of IPsec. Consult the manual page for more information.

To let firewalls properly track state for gif(4) tunnels too, you have to enable the `IPSEC_FILTERGIF` in your kernel configuration:

```
options   IPSEC_FILTERGIF  #filter ipsec packets from a tunnel
```

IPsec consists of two sub-protocols:

- *Encapsulated Security Payload (ESP)*, protects the IP packet data from third party interference,

by encrypting the contents using symmetric cryptography algorithms (like Blowfish, 3DES).

- *Authentication Header (AH)*, protects the IP packet header from third party interference and spoofing, by computing a cryptographic checksum and hashing the IP packet header fields with a secure hashing function. This is then followed by an additional header that contains the hash, to allow the information in the packet to be authenticated.

ESP and AH can either be used together or separately, depending on the environment.

IPsec can either be used to directly encrypt the traffic between two hosts (known as *Transport Mode*); or to build "virtual tunnels" between two subnets, which could be used for secure communication between two corporate networks (known as *Tunnel Mode*). The latter is more commonly known as a *Virtual Private Network (VPN)*. The ipsec(4) manual page should be consulted for detailed information on the IPsec subsystem in FreeBSD.

To add IPsec support to your kernel, add the following options to your kernel configuration file:

```
options   IPSEC         #IP security
options   IPSEC_ESP     #IP security (crypto; define w/ IPSEC)
```

If IPsec debugging support is desired, the following kernel option should also be added:

```
options   IPSEC_DEBUG  #debug for IP security
```

35.10.2. The Problem

There is no standard for what constitutes a VPN. VPNs can be implemented using a number of different technologies, each of which have their own strengths and weaknesses. This section presents a scenario, and the strategies used for implementing a VPN for this scenario.

35.10.3. The Scenario: Two networks, connected to the Internet, to behave as one

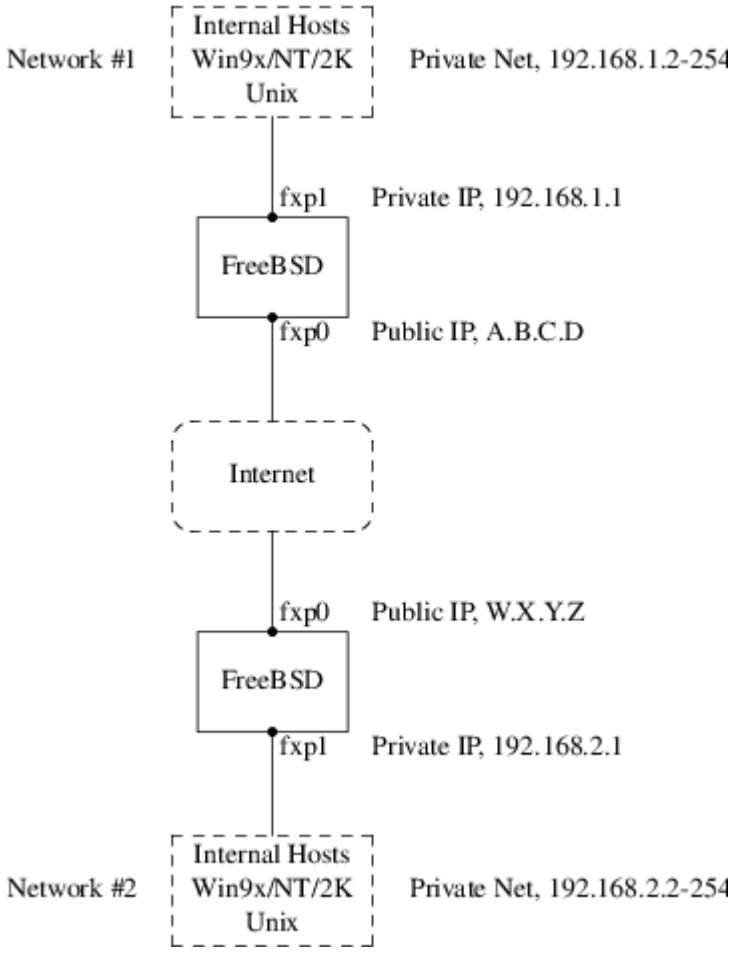
The premise is as follows:

- You have at least two sites
- Both sites are using IP internally
- Both sites are connected to the Internet, through a gateway that is running FreeBSD.
- The gateway on each network has at least one public IP address.
- The internal addresses of the two networks can be public or private IP addresses, it does not matter. You can be running NAT on the gateway machine if necessary.
- The internal IP addresses of the two networks *do not collide*. While I expect it is theoretically possible to use a combination of VPN technology and NAT to get this to work, I expect it to be a configuration nightmare.

If you find that you are trying to connect two networks, both of which, internally, use the same

private IP address range (e.g. both of them use `192.168.1.x`), then one of the networks will have to be renumbered.

The network topology might look something like this:



Notice the two public IP addresses. I will use the letters to refer to them in the rest of this article. Anywhere you see those letters in this article, replace them with your own public IP addresses. Note also that internally, the two gateway machines have .1 IP addresses, and that the two networks have different private IP addresses (`192.168.1.x` and `192.168.2.x` respectively). All the machines on the private networks have been configured to use the `.1` machine as their default gateway.

The intention is that, from a network point of view, each network should view the machines on the other network as though they were directly attached the same router — albeit a slightly slow router with an occasional tendency to drop packets.

This means that (for example), machine `192.168.1.20` should be able to run

```
ping 192.168.2.34
```

and have it work, transparently. Windows® machines should be able to see the machines on the other network, browse file shares, and so on, in exactly the same way that they can browse machines on the local network.

And the whole thing has to be secure. This means that traffic between the two networks has to be encrypted.

Creating a VPN between these two networks is a multi-step process. The stages are as follows:

1. Create a "virtual" network link between the two networks, across the Internet. Test it, using tools like ping(8), to make sure it works.
2. Apply security policies to ensure that traffic between the two networks is transparently encrypted and decrypted as necessary. Test this, using tools like tcpdump(1), to ensure that traffic is encrypted.
3. Configure additional software on the FreeBSD gateways, to allow Windows® machines to see one another across the VPN.

35.10.3.1. Step 1: Creating and testing a "virtual" network link

Suppose that you were logged in to the gateway machine on network #1 (with public IP address `A.B.C.D`, private IP address `192.168.1.1`), and you ran `ping 192.168.2.1`, which is the private address of the machine with IP address `W.X.Y.Z`. What needs to happen in order for this to work?

1. The gateway machine needs to know how to reach `192.168.2.1`. In other words, it needs to have a route to `192.168.2.1`.
2. Private IP addresses, such as those in the `192.168.x` range are not supposed to appear on the Internet at large. Instead, each packet you send to `192.168.2.1` will need to be wrapped up inside another packet. This packet will need to appear to be from `A.B.C.D`, and it will have to be sent to `W.X.Y.Z`. This process is called *encapsulation*.
3. Once this packet arrives at `W.X.Y.Z` it will need to "unencapsulated", and delivered to `192.168.2.1`.

You can think of this as requiring a "tunnel" between the two networks. The two "tunnel mouths" are the IP addresses `A.B.C.D` and `W.X.Y.Z`, and the tunnel must be told the addresses of the private IP addresses that will be allowed to pass through it. The tunnel is used to transfer traffic with private IP addresses across the public Internet.

This tunnel is created by using the generic interface, or gif devices on FreeBSD. As you can imagine, the gif interface on each gateway host must be configured with four IP addresses; two for the public IP addresses, and two for the private IP addresses.

Support for the gif device must be compiled in to the FreeBSD kernel on both machines. You can do this by adding the line:

```
device gif
```

to the kernel configuration files on both machines, and then compile, install, and reboot as normal.

Configuring the tunnel is a two step process. First the tunnel must be told what the outside (or public) IP addresses are, using ifconfig(8). Then the private IP addresses must be configured using ifconfig(8).

On the gateway machine on network #1 you would run the following commands to configure the tunnel.

```
# ifconfig gif0 create
# ifconfig gif0 tunnel A.B.C.D W.X.Y.Z
# ifconfig gif0 inet 192.168.1.1 192.168.2.1 netmask 0xffffffff
```

On the other gateway machine you run the same commands, but with the order of the IP addresses reversed.

```
# ifconfig gif0 create
# ifconfig gif0 tunnel W.X.Y.Z A.B.C.D
# ifconfig gif0 inet 192.168.2.1 192.168.1.1 netmask 0xffffffff
```

You can then run:

```
ifconfig gif0
```

to see the configuration. For example, on the network #1 gateway, you would see this:

```
# ifconfig gif0
gif0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1280
        tunnel inet A.B.C.D --> W.X.Y.Z
        inet 192.168.1.1 --> 192.168.2.1 netmask 0xffffffff
```

As you can see, a tunnel has been created between the physical addresses `A.B.C.D` and `W.X.Y.Z`, and the traffic allowed through the tunnel is that between `192.168.1.1` and `192.168.2.1`.

This will also have added an entry to the routing table on both machines, which you can examine with the command `netstat -rn`. This output is from the gateway host on network #1.

```
# netstat -rn
Routing tables

Internet:
Destination      Gateway       Flags    Refs    Use    Netif  Expire
...
192.168.2.1      192.168.1.1   UH        0        0    gif0
...
```

As the "Flags" value indicates, this is a host route, which means that each gateway knows how to reach the other gateway, but they do not know how to reach the rest of their respective networks. That problem will be fixed shortly.

It is likely that you are running a firewall on both machines. This will need to be circumvented for your VPN traffic. You might want to allow all traffic between both networks, or you might want to include firewall rules that protect both ends of the VPN from one another.

It greatly simplifies testing if you configure the firewall to allow all traffic through the VPN. You can always tighten things up later. If you are using ipfw(8) on the gateway machines then a command like

```
ipfw add 1 allow ip from any to any via gif0
```

will allow all traffic between the two end points of the VPN, without affecting your other firewall rules. Obviously you will need to run this command on both gateway hosts.

This is sufficient to allow each gateway machine to ping the other. On 192.168.1.1, you should be able to run

```
ping 192.168.2.1
```

and get a response, and you should be able to do the same thing on the other gateway machine.

However, you will not be able to reach internal machines on either network yet. This is because of the routing — although the gateway machines know how to reach one another, they do not know how to reach the network behind each one.

To solve this problem you must add a static route on each gateway machine. The command to do this on the first gateway would be:

```
route add 192.168.2.0 192.168.2.1 netmask 0xffffff00
```

This says "In order to reach the hosts on the network 192.168.2.0, send the packets to the host 192.168.2.1". You will need to run a similar command on the other gateway, but with the 192.168.1.x addresses instead.

IP traffic from hosts on one network will now be able to reach hosts on the other network.

That has now created two thirds of a VPN between the two networks, in as much as it is "virtual" and it is a "network". It is not private yet. You can test this using ping(8) and tcpdump(1). Log in to the gateway host and run

```
tcpdump dst host 192.168.2.1
```

In another log in session on the same host run

```
ping 192.168.2.1
```

You will see output that looks something like this:

```
16:10:24.018080 192.168.1.1  192.168.2.1: icmp: echo request
```

```
16:10:24.018109 192.168.1.1  192.168.2.1: icmp: echo reply
16:10:25.018814 192.168.1.1  192.168.2.1: icmp: echo request
16:10:25.018847 192.168.1.1  192.168.2.1: icmp: echo reply
16:10:26.028896 192.168.1.1  192.168.2.1: icmp: echo request
16:10:26.029112 192.168.1.1  192.168.2.1: icmp: echo reply
```

As you can see, the ICMP messages are going back and forth unencrypted. If you had used the `-s` parameter to tcpdump(1) to grab more bytes of data from the packets you would see more information.

Obviously this is unacceptable. The next section will discuss securing the link between the two networks so that all traffic is automatically encrypted.

Summary:

- Configure both kernels with "device gif".
- Edit /etc/rc.conf on gateway host #1 and add the following lines (replacing IP addresses as necessary).

```
gif_interfaces="gif0"
gifconfig_gif0="A.B.C.D W.X.Y.Z"
ifconfig_gif0="inet 192.168.1.1 192.168.2.1 netmask 0xffffffff"
static_routes="vpn"
route_vpn="192.168.2.0 192.168.2.1 netmask 0xffffff00"
```

- Edit your firewall script (/etc/rc.firewall, or similar) on both hosts, and add

```
ipfw add 1 allow ip from any to any via gif0
```

- Make similar changes to /etc/rc.conf on gateway host #2, reversing the order of IP addresses.

35.10.3.2. Step 2: Securing the link

To secure the link we will be using IPsec. IPsec provides a mechanism for two hosts to agree on an encryption key, and to then use this key in order to encrypt data between the two hosts.

The are two areas of configuration to be considered here.

1. There must be a mechanism for two hosts to agree on the encryption mechanism to use. Once two hosts have agreed on this mechanism there is said to be a "security association" between them.
2. There must be a mechanism for specifying which traffic should be encrypted. Obviously, you do not want to encrypt all your outgoing traffic — you only want to encrypt the traffic that is part of the VPN. The rules that you put in place to determine what traffic will be encrypted are called "security policies".

Security associations and security policies are both maintained by the kernel, and can be modified by userland programs. However, before you can do this you must configure the kernel to support

IPsec and the Encapsulated Security Payload (ESP) protocol. This is done by configuring a kernel with:

```
options IPSEC
options IPSEC_ESP
```

and recompiling, reinstalling, and rebooting. As before you will need to do this to the kernels on both of the gateway hosts.

You have two choices when it comes to setting up security associations. You can configure them by hand between two hosts, which entails choosing the encryption algorithm, encryption keys, and so forth, or you can use daemons that implement the Internet Key Exchange protocol (IKE) to do this for you.

I recommend the latter. Apart from anything else, it is easier to set up.

Editing and displaying security policies is carried out using setkey(8). By analogy, `setkey` is to the kernel's security policy tables as route(8) is to the kernel's routing tables. `setkey` can also display the current security associations, and to continue the analogy further, is akin to `netstat -r` in that respect.

There are a number of choices for daemons to manage security associations with FreeBSD. This article will describe how to use one of these, racoon - which is available from security/ipsec-tools in the FreeBSD Ports collection.

The racoon software must be run on both gateway hosts. On each host it is configured with the IP address of the other end of the VPN, and a secret key (which you choose, and must be the same on both gateways).

The two daemons then contact one another, confirm that they are who they say they are (by using the secret key that you configured). The daemons then generate a new secret key, and use this to encrypt the traffic over the VPN. They periodically change this secret, so that even if an attacker were to crack one of the keys (which is as theoretically close to unfeasible as it gets) it will not do them much good — by the time they have cracked the key the two daemons have chosen another one.

The configuration file for racoon is stored in ${PREFIX}/etc/racoon. You should find a configuration file there, which should not need to be changed too much. The other component of racoon's configuration, which you will need to change, is the "pre-shared key".

The default racoon configuration expects to find this in the file ${PREFIX}/etc/racoon/psk.txt. It is important to note that the pre-shared key is *not* the key that will be used to encrypt your traffic across the VPN link, it is simply a token that allows the key management daemons to trust one another.

psk.txt contains a line for each remote site you are dealing with. In this example, where there are two sites, each psk.txt file will contain one line (because each end of the VPN is only dealing with one other end).

On gateway host #1 this line should look like this:

```
W.X.Y.Z           secret
```

That is, the *public* IP address of the remote end, whitespace, and a text string that provides the secret. Obviously, you should not use "secret" as your key — the normal rules for choosing a password apply.

On gateway host #2 the line would look like this

```
A.B.C.D           secret
```

That is, the public IP address of the remote end, and the same secret key. psk.txt must be mode `0600` (i.e., only read/write to `root`) before racoon will run.

You must run racoon on both gateway machines. You will also need to add some firewall rules to allow the IKE traffic, which is carried over UDP to the ISAKMP (Internet Security Association Key Management Protocol) port. Again, this should be fairly early in your firewall ruleset.

```
ipfw add 1 allow udp from A.B.C.D to W.X.Y.Z isakmp
ipfw add 1 allow udp from W.X.Y.Z to A.B.C.D isakmp
```

Once racoon is running you can try pinging one gateway host from the other. The connection is still not encrypted, but racoon will then set up the security associations between the two hosts — this might take a moment, and you may see this as a short delay before the ping commands start responding.

Once the security association has been set up you can view it using setkey(8). Run

```
setkey -D
```

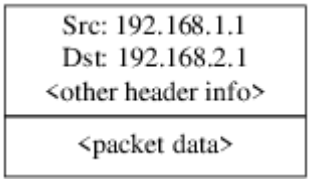
on either host to view the security association information.

That's one half of the problem. The other half is setting your security policies.

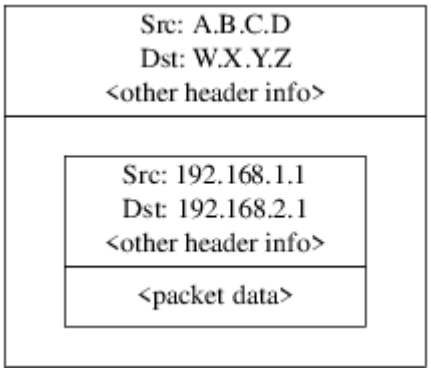
To create a sensible security policy, let's review what's been set up so far. This discussions hold for both ends of the link.

Each IP packet that you send out has a header that contains data about the packet. The header includes the IP addresses of both the source and destination. As we already know, private IP addresses, such as the `192.168.x.y` range are not supposed to appear on the public Internet. Instead, they must first be encapsulated inside another packet. This packet must have the public source and destination IP addresses substituted for the private addresses.

So if your outgoing packet started looking like this:



Then it will be encapsulated inside another packet, looking something like this:



This encapsulation is carried out by the gif device. As you can see, the packet now has real IP addresses on the outside, and our original packet has been wrapped up as data inside the packet that will be put out on the Internet.

Obviously, we want all traffic between the VPNs to be encrypted. You might try putting this in to words, as:

"If a packet leaves from `A.B.C.D`, and it is destined for `W.X.Y.Z`, then encrypt it, using the necessary security associations."

"If a packet arrives from `W.X.Y.Z`, and it is destined for `A.B.C.D`, then decrypt it, using the necessary security associations."

That's close, but not quite right. If you did this, all traffic to and from `W.X.Y.Z`, even traffic that was not part of the VPN, would be encrypted. That's not quite what you want. The correct policy is as follows

"If a packet leaves from `A.B.C.D`, and that packet is encapsulating another packet, and it is destined for `W.X.Y.Z`, then encrypt it, using the necessary security associations."

"If a packet arrives from `W.X.Y.Z`, and that packet is encapsulating another packet, and it is destined for `A.B.C.D`, then decrypt it, using the necessary security associations."

A subtle change, but a necessary one.

Security policies are also set using setkey(8). setkey(8) features a configuration language for defining the policy. You can either enter configuration instructions via stdin, or you can use the `-f` option to specify a filename that contains configuration instructions.

The configuration on gateway host #1 (which has the public IP address `A.B.C.D`) to force all outbound traffic to `W.X.Y.Z` to be encrypted is:

```
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P out ipsec esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

Put these commands in a file (e.g. /etc/ipsec.conf) and then run

```
# setkey -f /etc/ipsec.conf
```

`spdadd` tells setkey(8) that we want to add a rule to the secure policy database. The rest of this line specifies which packets will match this policy. `A.B.C.D/32` and `W.X.Y.Z/32` are the IP addresses and netmasks that identify the network or hosts that this policy will apply to. In this case, we want it to apply to traffic between these two hosts. `ipencap` tells the kernel that this policy should only apply to packets that encapsulate other packets. `-P out` says that this policy applies to outgoing packets, and `ipsec` says that the packet will be secured.

The second line specifies how this packet will be encrypted. `esp` is the protocol that will be used, while `tunnel` indicates that the packet will be further encapsulated in an IPsec packet. The repeated use of `A.B.C.D` and `W.X.Y.Z` is used to select the security association to use, and the final `require` mandates that packets must be encrypted if they match this rule.

This rule only matches outgoing packets. You will need a similar rule to match incoming packets.

```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P in ipsec esp/tunnel/W.X.Y.Z-A.B.C.D/require;
```

Note the `in` instead of `out` in this case, and the necessary reversal of the IP addresses.

The other gateway host (which has the public IP address `W.X.Y.Z`) will need similar rules.

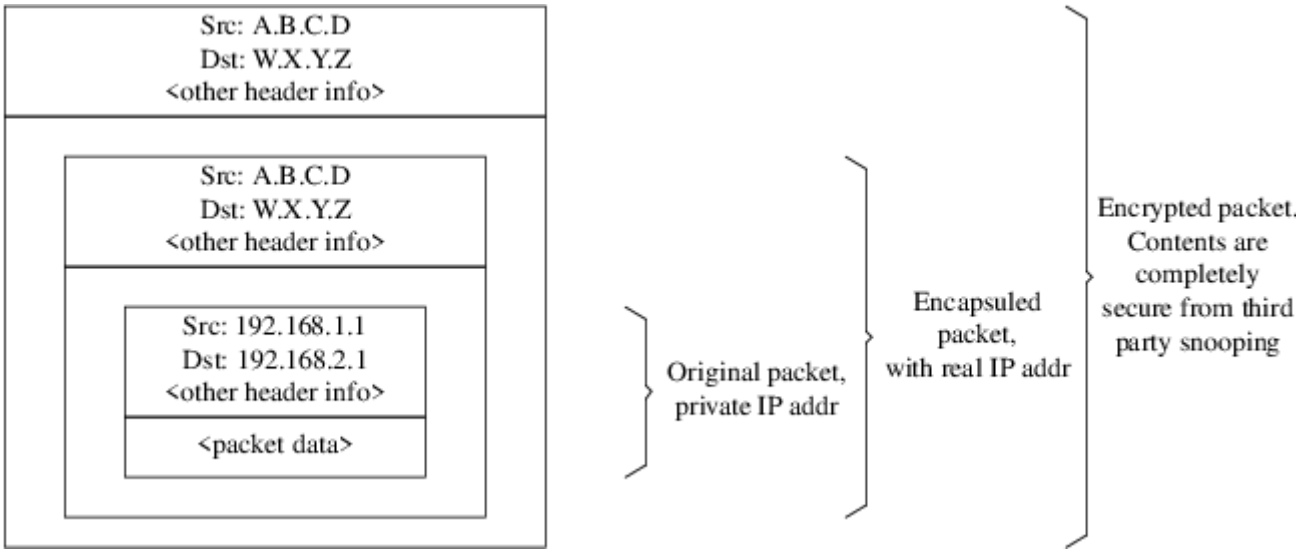
```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P out ipsec esp/tunnel/W.X.Y.Z-A.B.C.D/require;
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P in ipsec esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

Finally, you need to add firewall rules to allow ESP and IPENCAP packets back and forth. These rules will need to be added to both hosts.

```
ipfw add 1 allow esp from A.B.C.D to W.X.Y.Z
ipfw add 1 allow esp from W.X.Y.Z to A.B.C.D
ipfw add 1 allow ipencap from A.B.C.D to W.X.Y.Z
ipfw add 1 allow ipencap from W.X.Y.Z to A.B.C.D
```

Because the rules are symmetric you can use the same rules on each gateway host.

Outgoing packets will now look something like this:



When they are received by the far end of the VPN they will first be decrypted (using the security associations that have been negotiated by racoon). Then they will enter the gif interface, which will unwrap the second layer, until you are left with the innermost packet, which can then travel in to the inner network.

You can check the security using the same ping(8) test from earlier. First, log in to the `A.B.C.D` gateway machine, and run:

```
tcpdump dst host 192.168.2.1
```

In another log in session on the same host run

```
ping 192.168.2.1
```

This time you should see output like the following:

```
XXX tcpdump output
```

Now, as you can see, tcpdump(1) shows the ESP packets. If you try to examine them with the `-s` option you will see (apparently) gibberish, because of the encryption.

Congratulations. You have just set up a VPN between two remote sites.

Summary

- Configure both kernels with:

  ```
  options IPSEC
  options IPSEC_ESP
  ```

- Install security/ipsec-tools. Edit ${PREFIX}/etc/racoon/psk.txt on both gateway hosts, adding an entry for the remote host's IP address and a secret key that they both know. Make sure this file

is mode 0600.

- Add the following lines to /etc/rc.conf on each host:

```
ipsec_enable="YES"
ipsec_file="/etc/ipsec.conf"
```

- Create an /etc/ipsec.conf on each host that contains the necessary spdadd lines. On gateway host #1 this would be:

```
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P out ipsec
  esp/tunnel/A.B.C.D-W.X.Y.Z/require;
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P in ipsec
  esp/tunnel/W.X.Y.Z-A.B.C.D/require;
```

  On gateway host #2 this would be:

```
spdadd W.X.Y.Z/32 A.B.C.D/32 ipencap -P out ipsec
  esp/tunnel/W.X.Y.Z-A.B.C.D/require;
spdadd A.B.C.D/32 W.X.Y.Z/32 ipencap -P in ipsec
  esp/tunnel/A.B.C.D-W.X.Y.Z/require;
```

- Add firewall rules to allow IKE, ESP, and IPENCAP traffic to both hosts:

```
ipfw add 1 allow udp from A.B.C.D to W.X.Y.Z isakmp
ipfw add 1 allow udp from W.X.Y.Z to A.B.C.D isakmp
ipfw add 1 allow esp from A.B.C.D to W.X.Y.Z
ipfw add 1 allow esp from W.X.Y.Z to A.B.C.D
ipfw add 1 allow ipencap from A.B.C.D to W.X.Y.Z
ipfw add 1 allow ipencap from W.X.Y.Z to A.B.C.D
```

The previous two steps should suffice to get the VPN up and running. Machines on each network will be able to refer to one another using IP addresses, and all traffic across the link will be automatically and securely encrypted.

35.11. OpenSSH

OpenSSH is a set of network connectivity tools used to access remote machines securely. It can be used as a direct replacement for `rlogin`, `rsh`, `rcp`, and `telnet`. Additionally, TCP/IP connections can be tunneled/forwarded securely through SSH. OpenSSH encrypts all traffic to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

OpenSSH is maintained by the OpenBSD project, and is based upon SSH v1.2.12 with all the recent bug fixes and updates. It is compatible with both SSH protocols 1 and 2.

35.11.1. Advantages of Using OpenSSH

Normally, when using telnet(1) or rlogin(1), data is sent over the network in an clear, un-encrypted form. Network sniffers anywhere in between the client and server can steal your user/password information or data transferred in your session. OpenSSH offers a variety of authentication and encryption methods to prevent this from happening.

35.11.2. Enabling sshd

The sshd is an option presented during a `Standard` install of FreeBSD. To see if sshd is enabled, check the rc.conf file for:

```
sshd_enable="YES"
```

This will load sshd(8), the daemon program for OpenSSH, the next time your system initializes. Alternatively, it is possible to use /etc/rc.d/sshd rc(8) script to start OpenSSH:

```
/etc/rc.d/sshd start
```

35.11.3. SSH Client

The ssh(1) utility works similarly to rlogin(1).

```
# ssh user@example.com
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host 'example.com' added to the list of known hosts.
user@example.com's password: *******
```

The login will continue just as it would have if a session was created using `rlogin` or `telnet`. SSH utilizes a key fingerprint system for verifying the authenticity of the server when the client connects. The user is prompted to enter `yes` only when connecting for the first time. Future attempts to login are all verified against the saved fingerprint key. The SSH client will alert you if the saved fingerprint differs from the received fingerprint on future login attempts. The fingerprints are saved in ~/.ssh/known_hosts, or ~/.ssh/known_hosts2 for SSH v2 fingerprints.

By default, recent versions of the OpenSSH servers only accept SSH v2 connections. The client will use version 2 if possible and will fall back to version 1. The client can also be forced to use one or the other by passing it the `-1` or `-2` for version 1 or version 2, respectively. The version 1 compatibility is maintained in the client for backwards compatibility with older versions.

35.11.4. Secure Copy

The scp(1) command works similarly to rcp(1); it copies a file to or from a remote machine, except in a secure fashion.

```
#  scp user@example.com:/COPYRIGHT COPYRIGHT
user@example.com's password: *******
COPYRIGHT            100% |*****************************|  4735
00:00
#
```

Since the fingerprint was already saved for this host in the previous example, it is verified when using scp(1) here.

The arguments passed to scp(1) are similar to cp(1), with the file or files in the first argument, and the destination in the second. Since the file is fetched over the network, through SSH, one or more of the file arguments takes on the form `user@host:path_to_remote_file`.

35.11.5. Configuration

The system-wide configuration files for both the OpenSSH daemon and client reside within the /etc/ssh directory.

ssh_config configures the client settings, while sshd_config configures the daemon.

Additionally, the `sshd_program` (/usr/sbin/sshd by default), and `sshd_flags`rc.conf options can provide more levels of configuration.

35.11.6. ssh-keygen

Instead of using passwords, ssh-keygen(1) can be used to generate DSA or RSA keys to authenticate a user:

```
% ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/user/.ssh/id_dsa):
Created directory '/home/user/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/user/.ssh/id_dsa.
Your public key has been saved in /home/user/.ssh/id_dsa.pub.
The key fingerprint is:
bb:48:db:f2:93:57:80:b6:aa:bc:f5:d5:ba:8f:79:17 user@host.example.com
```

ssh-keygen(1) will create a public and private key pair for use in authentication. The private key is stored in ~/.ssh/id_dsa or ~/.ssh/id_rsa, whereas the public key is stored in ~/.ssh/id_dsa.pub or ~/.ssh/id_rsa.pub, respectively for DSA and RSA key types. The public key must be placed in ~/.ssh/authorized_keys of the remote machine in order for the setup to work. Similarly, RSA version 1 public keys should be placed in ~/.ssh/authorized_keys.

This will allow connection to the remote machine based upon SSH keys instead of passwords.

If a passphrase is used in ssh-keygen(1), the user will be prompted for a password each time in

order to use the private key. ssh-agent(1) can alleviate the strain of repeatedly entering long passphrases, and is explored in the ssh-agent and ssh-add section below.

The various options and files can be different according to the OpenSSH version you have on your system; to avoid problems you should consult the ssh-keygen(1) manual page.

35.11.7. ssh-agent and ssh-add

The ssh-agent(1) and ssh-add(1) utilities provide methods for SSH keys to be loaded into memory for use, without needing to type the passphrase each time.

The ssh-agent(1) utility will handle the authentication using the private key(s) that are loaded into it. ssh-agent(1) should be used to launch another application. At the most basic level, it could spawn a shell or at a more advanced level, a window manager.

To use ssh-agent(1) in a shell, first it will need to be spawned with a shell as an argument. Secondly, the identity needs to be added by running ssh-add(1) and providing it the passphrase for the private key. Once these steps have been completed the user will be able to ssh(1) to any host that has the corresponding public key installed. For example:

```
% ssh-agent csh
% ssh-add
Enter passphrase for /home/user/.ssh/id_dsa:
Identity added: /home/user/.ssh/id_dsa (/home/user/.ssh/id_dsa)
%
```

To use ssh-agent(1) in X11, a call to ssh-agent(1) will need to be placed in ~/.xinitrc. This will provide the ssh-agent(1) services to all programs launched in X11. An example ~/.xinitrc file might look like this:

```
exec ssh-agent startxfce4
```

This would launch ssh-agent(1), which would in turn launch XFCE, every time X11 starts. Then once that is done and X11 has been restarted so that the changes can take effect, simply run ssh-add(1) to load all of your SSH keys.

35.11.8. SSH Tunneling

OpenSSH has the ability to create a tunnel to encapsulate another protocol in an encrypted session.

The following command tells ssh(1) to create a tunnel for telnet:

```
% ssh -2 -N -f -L 5023:localhost:23 user@foo.example.com
%
```

The `ssh` command is used with the following options:

`-2`

Forces `ssh` to use version 2 of the protocol. (Do not use if you are working with older SSH servers)

`-N`

Indicates no command, or tunnel only. If omitted, `ssh` would initiate a normal session.

`-f`

Forces `ssh` to run in the background.

`-L`

Indicates a local tunnel in *localport:remotehost:remoteport* fashion.

`user@foo.example.com`

The remote SSH server.

An SSH tunnel works by creating a listen socket on `localhost` on the specified port. It then forwards any connection received on the local host/port via the SSH connection to the specified remote host and port.

In the example, port *5023* on `localhost` is being forwarded to port *23* on `localhost` of the remote machine. Since *23* is telnet, this would create a secure telnet session through an SSH tunnel.

This can be used to wrap any number of insecure TCP protocols such as SMTP, POP3, FTP, etc.

Παράδειγμα 11. Using SSH to Create a Secure Tunnel for SMTP

```
% ssh -2 -N -f -L 5025:localhost:25 user@mailserver.example.com
user@mailserver.example.com's password: *****
% telnet localhost 5025
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mailserver.example.com ESMTP
```

This can be used in conjunction with an ssh-keygen(1) and additional user accounts to create a more seamless/hassle-free SSH tunneling environment. Keys can be used in place of typing a password, and the tunnels can be run as a separate user.

35.11.8.1. Practical SSH Tunneling Examples

35.11.8.1.1. Secure Access of a POP3 Server

At work, there is an SSH server that accepts connections from the outside. On the same office network resides a mail server running a POP3 server. The network, or network path between your home and office may or may not be completely trustable. Because of this, you need to check your e-

mail in a secure manner. The solution is to create an SSH connection to your office's SSH server, and tunnel through to the mail server.

```
% ssh -2 -N -f -L 2110:mail.example.com:110 user@ssh-server.example.com
user@ssh-server.example.com's password: ******
```

When the tunnel is up and running, you can point your mail client to send POP3 requests to `localhost` port 2110. A connection here will be forwarded securely across the tunnel to `mail.example.com`.

35.11.8.1.2. Bypassing a Draconian Firewall

Some network administrators impose extremely draconian firewall rules, filtering not only incoming connections, but outgoing connections. You may be only given access to contact remote machines on ports 22 and 80 for SSH and web surfing.

You may wish to access another (perhaps non-work related) service, such as an Ogg Vorbis server to stream music. If this Ogg Vorbis server is streaming on some other port than 22 or 80, you will not be able to access it.

The solution is to create an SSH connection to a machine outside of your network's firewall, and use it to tunnel to the Ogg Vorbis server.

```
% ssh -2 -N -f -L 8888:music.example.com:8000 user@unfirewalled-system.example.org
user@unfirewalled-system.example.org's password: *******
```

Your streaming client can now be pointed to `localhost` port 8888, which will be forwarded over to `music.example.com` port 8000, successfully evading the firewall.

35.11.9. The `AllowUsers` Users Option

It is often a good idea to limit which users can log in and from where. The `AllowUsers` option is a good way to accomplish this. For example, to only allow the `root` user to log in from `192.168.1.32`, something like this would be appropriate in the /etc/ssh/sshd_config file:

```
AllowUsers root@192.168.1.32
```

To allow the user `admin` to log in from anywhere, just list the username by itself:

```
AllowUsers admin
```

Multiple users should be listed on the same line, like so:

```
AllowUsers root@192.168.1.32 admin
```

It is important that you list each user that needs to log in to this machine; otherwise they will be locked out.

After making changes to /etc/ssh/sshd_config you must tell sshd(8) to reload its config files, by running:

```
# /etc/rc.d/sshd reload
```

35.11.10. Further Reading

OpenSSH

ssh(1) scp(1) ssh-keygen(1) ssh-agent(1) ssh-add(1) ssh_config(5)

sshd(8) sftp-server(8) sshd_config(5)

35.12. File System Access Control Lists

In conjunction with file system enhancements like snapshots, FreeBSD 5.0 and later offers the security of File System Access Control Lists (ACLs).

Access Control Lists extend the standard UNIX® permission model in a highly compatible (POSIX®.1e) way. This feature permits an administrator to make use of and take advantage of a more sophisticated security model.

To enable ACL support for UFS file systems, the following:

```
options UFS_ACL
```

must be compiled into the kernel. If this option has not been compiled in, a warning message will be displayed when attempting to mount a file system supporting ACLs. This option is included in the GENERIC kernel. ACLs rely on extended attributes being enabled on the file system. Extended attributes are natively supported in the next generation UNIX® file system, UFS2.

A higher level of administrative overhead is required to configure extended attributes on UFS1 than on UFS2. The performance of extended attributes on UFS2 is also substantially higher. As a result, UFS2 is generally recommended in preference to UFS1 for use with access control lists.

ACLs are enabled by the mount-time administrative flag, `acls`, which may be added to /etc/fstab. The mount-time flag can also be automatically set in a persistent manner using tunefs(8) to modify a superblock ACLs flag in the file system header. In general, it is preferred to use the superblock flag for several reasons:

- The mount-time ACLs flag cannot be changed by a remount (mount(8) `-u`), only by means of a complete umount(8) and fresh mount(8). This means that ACLs cannot be enabled on the root

file system after boot. It also means that you cannot change the disposition of a file system once it is in use.

- Setting the superblock flag will cause the file system to always be mounted with ACLs enabled even if there is not an fstab entry or if the devices re-order. This prevents accidental mounting of the file system without ACLs enabled, which can result in ACLs being improperly enforced, and hence security problems.

We may change the ACLs behavior to allow the flag to be enabled without a complete fresh mount(8), but we consider it desirable to discourage accidental mounting without ACLs enabled, because you can shoot your feet quite nastily if you enable ACLs, then disable them, then re-enable them without flushing the extended attributes. In general, once you have enabled ACLs on a file system, they should not be disabled, as the resulting file protections may not be compatible with those intended by the users of the system, and re-enabling ACLs may re-attach the previous ACLs to files that have since had their permissions changed, resulting in other unpredictable behavior.

File systems with ACLs enabled will show a + (plus) sign in their permission settings when viewed. For example:

```
drwx------  2 robert  robert  512 Dec 27 11:54 private
drwxrwx---+ 2 robert  robert  512 Dec 23 10:57 directory1
drwxrwx---+ 2 robert  robert  512 Dec 22 10:20 directory2
drwxrwx---+ 2 robert  robert  512 Dec 27 11:57 directory3
drwxr-xr-x  2 robert  robert  512 Nov 10 11:54 public_html
```

Here we see that the directory1, directory2, and directory3 directories are all taking advantage of ACLs. The public_html directory is not.

35.12.1. Making Use of ACLs

The file system ACLs can be viewed by the getfacl(1) utility. For instance, to view the ACL settings on the test file, one would use the command:

```
% getfacl test
    #file:test
    #owner:1001
    #group:1001
    user::rw-
    group::r--
    other::r--
```

To change the ACL settings on this file, invoke the setfacl(1) utility. Observe:

```
% setfacl -k test
```

The `-k` flag will remove all of the currently defined ACLs from a file or file system. The more preferable method would be to use `-b` as it leaves the basic fields required for ACLs to work.

```
% setfacl -m u:trhodes:rwx,group:web:r--,o::--- test
```

In the aforementioned command, the `-m` option was used to modify the default ACL entries. Since there were no pre-defined entries, as they were removed by the previous command, this will restore the default options and assign the options listed. Take care to notice that if you add a user or group which does not exist on the system, an `Invalid argument` error will be printed to stdout.

35.13. Monitoring Third Party Security Issues

In recent years, the security world has made many improvements to how vulnerability assessment is handled. The threat of system intrusion increases as third party utilities are installed and configured for virtually any operating system available today.

Vulnerability assessment is a key factor in security, and while FreeBSD releases advisories for the base system, doing so for every third party utility is beyond the FreeBSD Project's capability. There is a way to mitigate third party vulnerabilities and warn administrators of known security issues. A FreeBSD add on utility known as Portaudit exists solely for this purpose.

The ports-mgmt/portaudit port polls a database, updated and maintained by the FreeBSD Security Team and ports developers, for known security issues.

To begin using Portaudit, one must install it from the Ports Collection:

```
# cd /usr/ports/ports-mgmt/portaudit  make install clean
```

During the install process, the configuration files for periodic(8) will be updated, permitting Portaudit output in the daily security runs. Ensure the daily security run emails, which are sent to `root`'s email account, are being read. No more configuration will be required here.

After installation, an administrator can update the database and view known vulnerabilities in installed packages by invoking the following command:

```
# portaudit -Fda
```

The database will automatically be updated during the periodic(8) run; thus, the previous command is completely optional. It is only required for the following examples.

To audit the third party utilities installed as part of the Ports Collection at anytime, an administrator need only run the following command:

```
# portaudit -a
```

Portaudit will produce something like this for vulnerable packages:

```
Affected package: cups-base-1.1.22.0_1
Type of problem: cups-base -- HPGL buffer overflow vulnerability.
Reference: http://www.FreeBSD.org/ports/portaudit/40a3bca2-6809-11d9-a9e7-
0001020eed82.html

1 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s) immediately.
```

By pointing a web browser to the URL shown, an administrator may obtain more information about the vulnerability in question. This will include versions affected, by FreeBSD Port version, along with other web sites which may contain security advisories.

In short, Portaudit is a powerful utility and extremely useful when coupled with the Portupgrade port.

35.14. FreeBSD Security Advisories

Like many production quality operating systems, FreeBSD publishes "Security Advisories". These advisories are usually mailed to the security lists and noted in the Errata only after the appropriate releases have been patched. This section will work to explain what an advisory is, how to understand it, and what measures to take in order to patch a system.

35.14.1. What does an advisory look like?

The FreeBSD security advisories look similar to the one below, taken from the ηλεκτρονική λίστα Ανακοινώσεων για Θέματα Ασφάλειας του FreeBSD mailing list.

```
=============================================================================
FreeBSD-SA-XX:XX.UTIL                                          Security Advisory
                                                               The FreeBSD Project

Topic:          denial of service due to some problem ①

Category:       core ②
Module:         sys ③
Announced:      2003-09-23 ④
Credits:        Person@EMAIL-ADDRESS ⑤
Affects:        All releases of FreeBSD ⑥
                FreeBSD 4-STABLE prior to the correction date
Corrected:      2003-09-23 16:42:59 UTC (RELENG_4, 4.9-PRERELEASE)
                2003-09-23 20:08:42 UTC (RELENG_5_1, 5.1-RELEASE-p6)
                2003-09-23 20:07:06 UTC (RELENG_5_0, 5.0-RELEASE-p15)
```

```
                2003-09-23 16:44:58 UTC (RELENG_4_8, 4.8-RELEASE-p8)
                2003-09-23 16:47:34 UTC (RELENG_4_7, 4.7-RELEASE-p18)
                2003-09-23 16:49:46 UTC (RELENG_4_6, 4.6-RELEASE-p21)
                2003-09-23 16:51:24 UTC (RELENG_4_5, 4.5-RELEASE-p33)
                2003-09-23 16:52:45 UTC (RELENG_4_4, 4.4-RELEASE-p43)
                2003-09-23 16:54:39 UTC (RELENG_4_3, 4.3-RELEASE-p39) ⑦
CVE Name:   CVE-XXXX-XXXX ⑧

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit
http://www.FreeBSD.org/security/.

I.   Background ⑨

II.  Problem Description ⑩

III. Impact ⑪

IV.  Workaround ⑫

V.   Solution ⑬

VI.  Correction details ⑭

VII. References ⑮
```

① The `Topic` field indicates exactly what the problem is. It is basically an introduction to the current security advisory and notes the utility with the vulnerability.

② The `Category` refers to the affected part of the system which may be one of `core`, `contrib`, or `ports`. The `core` category means that the vulnerability affects a core component of the FreeBSD operating system. The `contrib` category means that the vulnerability affects software contributed to the FreeBSD Project, such as sendmail. Finally the `ports` category indicates that the vulnerability affects add on software available as part of the Ports Collection.

③ The `Module` field refers to the component location, for instance `sys`. In this example, we see that the module, `sys`, is affected; therefore, this vulnerability affects a component used within the kernel.

④ The `Announced` field reflects the date said security advisory was published, or announced to the world. This means that the security team has verified that the problem does exist and that a patch has been committed to the FreeBSD source code repository.

⑤ The `Credits` field gives credit to the individual or organization who noticed the vulnerability and reported it.

⑥ The `Affects` field explains which releases of FreeBSD are affected by this vulnerability. For the kernel, a quick look over the output from `ident` on the affected files will help in determining the revision. For ports, the version number is listed after the port name in /var/db/pkg. If the system does not sync with the FreeBSD CVS repository and rebuild daily, chances are that it is affected.

⑦ The `Corrected` field indicates the date, time, time offset, and release that was corrected. Reserved

for the identification information used to look up vulnerabilities in the Common Vulnerabilities Database system.

⑧ The `Background` field gives information on exactly what the affected utility is. Most of the time this is why the utility exists in FreeBSD, what it is used for, and a bit of information on how the utility came to be.

⑨ The `Problem Description` field explains the security hole in depth. This can include information on flawed code, or even how the utility could be maliciously used to open a security hole.

⑩ The `Impact` field describes what type of impact the problem could have on a system. For example, this could be anything from a denial of service attack, to extra privileges available to users, or even giving the attacker superuser access.

⑪ The `Workaround` field offers a feasible workaround to system administrators who may be incapable of upgrading the system. This may be due to time constraints, network availability, or a slew of other reasons. Regardless, security should not be taken lightly, and an affected system should either be patched or the security hole workaround should be implemented.

⑫ The `Solution` field offers instructions on patching the affected system. This is a step by step tested and verified method for getting a system patched and working securely.

⑬ The `Correction Details` field displays the CVS branch or release name with the periods changed to underscore characters. It also shows the revision number of the affected files within each branch.

⑭ The `References` field usually offers sources of other information. This can include web URLs, books, mailing lists, and newsgroups.

35.15. Process Accounting

Process accounting is a security method in which an administrator may keep track of system resources used, their allocation among users, provide for system monitoring, and minimally track a user's commands.

This indeed has its own positive and negative points. One of the positives is that an intrusion may be narrowed down to the point of entry. A negative is the amount of logs generated by process accounting, and the disk space they may require. This section will walk an administrator through the basics of process accounting.

35.15.1. Enable and Utilizing Process Accounting

Before making use of process accounting, it must be enabled. To do this, execute the following commands:

```
# touch /var/account/acct

# accton /var/account/acct

# echo 'accounting_enable="YES"' >> /etc/rc.conf
```

Once enabled, accounting will begin to track CPU stats, commands, etc. All accounting logs are in a non-human readable format and may be viewed using the sa(8) utility. If issued without any options, `sa` will print information relating to the number of per user calls, the total elapsed time in minutes, total CPU and user time in minutes, average number of I/O operations, etc.

To view information about commands being issued, one would use the lastcomm(1) utility. The `lastcomm` may be used to print out commands issued by users on specific ttys(5), for example:

```
# lastcomm ls
    trhodes ttyp1
```

Would print out all known usage of the `ls` by `trhodes` on the ttyp1 terminal.

Many other useful options exist and are explained in the lastcomm(1), acct(5) and sa(8) manual pages.

Chapter 36. Jails

36.1. Σύνοψη

Το κεφάλαιο αυτό εξηγεί τι είναι τα jails (φυλακές) του FreeBSD και πως χρησιμοποιούνται. Τα jails, που αναφέρονται ορισμένες φορές σαν μια ενισχυμένη εναλλακτική λύση για *περιβάλλοντα chroot*, είναι ένα ισχυρό εργαλείο για διαχειριστές συστημάτων, αλλά η βασική τους χρήση μπορεί επίσης να είναι χρήσιμη σε προχωρημένους χρήστες.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τι είναι ένα jail και τι σκοπό μπορεί να εξυπηρετήσει σε εγκαταστάσεις FreeBSD.
- Πως να φτιάξετε, να εκκινήσετε, και να σταματήσετε ένα jail.
- Τα βασικά της διαχείρισης ενός jail, τόσο μέσα, όσο και έξω από αυτό.

Άλλες πηγές χρήσιμων πληροφοριών σχετικά με τα jails είναι:

- Η σελίδα manual του jail(8). Περιέχει πλήρη αναφορά του βοηθητικού προγράμματος `jail` - του διαχειριστικού εργαλείου που μπορεί να χρησιμοποιηθεί στο FreeBSD για την εκκίνηση, διακοπή, και έλεγχο των jails.
- Οι λίστες ταχυδρομείου και τα αρχεία τους. Τα αρχεία από την ηλεκτρονική λίστα γενικών ερωτήσεων του FreeBSD και άλλες λίστες που εξυπηρετούνται από τον εξυπηρετητής για ηλεκτρονικές λίστες του FreeBSD περιέχουν πλήρη οδηγό για τα jails. Είναι πάντοτε ενδιαφέρον να ψάχνετε τα αρχεία ή να δημοσιεύετε νέες ερωτήσεις στη λίστα freebsd-questions.

36.2. Όροι των Jails

Για να κατανοήσετε καλύτερα το πως οι εσωτερικές λειτουργίες του FreeBSD σχετίζονται με τα jails και πως αυτές αλληλεπιδρούν με τα υπόλοιπα μέρη του FreeBSD, θα χρησιμοποιήσουμε εκτενώς τους παρακάτω όρους:

chroot(8) (εντολή)

Ένα βοηθητικό πρόγραμμα, το οποίο χρησιμοποιεί την κλήση συστήματος chroot(2) του FreeBSD για να αλλάξει τον γονικό κατάλογο (root directory) μιας διεργασίας και όλων των άλλων διεργασιών που εξαρτώνται από αυτή.

chroot(2) (περιβάλλον)

Το περιβάλλον μια διεργασίας που τρέχει μέσα σε ένα "chroot". Αυτό περιλαμβάνει πόρους όπως το τμήμα του συστήματος αρχείων που είναι ορατό, τα ID του χρήστη και της ομάδας που είναι διαθέσιμα, καθώς και τις διεπαφές δικτύου (network interfaces), τους μηχανισμούς IPC κλπ.

jail(8) (εντολή)

Το πρόγραμμα που σας επιτρέπει να διαχειρίζεστε το σύστημα σας και να ξεκινάτε διεργασίες σε περιβάλλον jail.

host (σύστημα (system), διεργασία (process), χρήστης (user), κλπ.)

Το φυσικό σύστημα που φιλοξενεί και ελέγχει ένα περιβάλλον jail. Το host system έχει πρόσβαση σε όλο το διαθέσιμο υλικό, και μπορεί να ελέγξει διεργασίες τόσο μέσα όσο και έξω από το περιβάλλον του jail. Μία από τις σημαντικότερες διαφορές μεταξύ του host system και του jail είναι ότι οι περιορισμοί που εφαρμόζονται στις διεργασίες του χρήστη root μέσα στο περιβάλλον jail, δεν ισχύουν για τις διεργασίες στο host system.

hosted (σύστημα (system), διεργασία (process), χρήστης (user), κλπ.)

Μια διεργασία, ένας χρήστης ή κάποια άλλη οντότητα, του οποίου η πρόσβαση στους πόρους του συστήματος περιορίζεται μέσα από ένα jail.

36.3. Εισαγωγή

Μια και η διαχείριση ενός συστήματος μπορεί να είναι δύσκολη και περίπλοκη, αναπτύχθηκαν αρκετά εργαλεία τα οποία μπορούν να κάνουν τη ζωή ενός διαχειριστή πολύ πιο εύκολη. Τα εργαλεία αυτά προσφέρουν κάποιες πρόσθετες δυνατότητες όσο αφορά τον τρόπο εγκατάστασης, ρύθμισης και συντήρησης ενός συστήματος. Μια από τις εργασίες που αναμένεται να εκτελέσει κάθε διαχειριστής συστήματος, είναι να ρυθμίσει σωστά την ασφάλεια του συστήματος, προκειμένου να προσφέρει τις υπηρεσίες για τις οποίες έχει προγραμματιστεί, χωρίς να επιτρέπει συμβιβασμούς στην ασφάλεια.

Ένα από τα εργαλεία που μπορούν να ενισχύσουν την ασφάλεια ενός συστήματος FreeBSD είναι τα *jails*. Τα Jails πρωτοεμφανίστηκαν στο FreeBSD 4.X από τον Poul-Henning Kamp <phk@FreeBSD.org>, αλλά βελτιώθηκαν πολύ περισσότερο στην έκδοση FreeBSD 5.X, προκειμένου να προσφέρουν περισσότερες δυνατότητες και να είναι περισσότερο ευέλικτα. Η ανάπτυξή τους συνεχίζεται ακόμη, με βελτιώσεις στους τομείς της ευχρηστίας, της απόδοσης, της αξιοπιστίας και της ασφάλειας που πρέπει να παρέχουν.

36.3.1. Τι Είναι Ένα Jail

Τα λειτουργικά συστήματα τύπου BSD, παρείχαν το chroot(2) από την εποχή του 4.2BSD. Η εντολή chroot(8) μπορεί να χρησιμοποιηθεί για να αλλάξει τον γονικό κατάλογο μιας ομάδας διεργασιών, δημιουργώντας ένα ασφαλές περιβάλλον, ξεχωριστό από το υπόλοιπο σύστημα. Όσες διεργασίες δημιουργούνται σε έναν τέτοιο περιβάλλον, δεν έχουν πρόσβαση σε αρχεία και πόρους έξω από αυτό. Για αυτό το λόγο, αν μια υπηρεσία τρέχει μέσα σε ένα τέτοιο περιβάλλον, και κάποιος εισβολέας καταφέρει να διεισδύσει σε αυτή, δε θα του επιτραπεί η πρόσβαση στο υπόλοιπο σύστημα. Η εντολή chroot(8) είναι πολύ καλή για απλές εργασίες οι οποίες δε χρειάζονται να είναι πολύ ευέλικτες ή να διαθέτουν πολύπλοκα και προηγμένα χαρακτηριστικά. Ωστόσο, από την αρχή της ιδέας του chroot, βρέθηκαν αρκετοί τρόποι για να μπορέσει κάποιος να ξεφύγει από το περιβάλλον αυτό. Παρ' όλο που έχουν διορθωθεί πολλά σφάλματα στις πρόσφατες εκδόσεις του πυρήνα του FreeBSD, ήταν ξεκάθαρο ότι η chroot(2) δεν ήταν η ιδανική λύση για την ασφάλιση υπηρεσιών. Έπρεπε να υλοποιηθεί ένα νέο υποσύστημα.

Αυτός είναι ένας από τους κύριους λόγους για την ανάπτυξη των *jails*.

Τα jails βελτίωσαν με διάφορους τρόπους την ιδέα του παραδοσιακού περιβάλλοντος του chroot(2). Στο τυπικό περιβάλλον του chroot(2), οι διεργασίες περιορίζονται μόνος ως προς το μέρος του συστήματος αρχείων όπου μπορούν να έχουν πρόσβαση. Οι υπόλοιποι πόροι του συστήματος (όπως

οι χρήστες, οι τρέχοντες διεργασίες, το υποσύστημα δικτύωσης) είναι κοινόχρηστοι μεταξύ των διεργασιών του περιβάλλοντος chroot και των διεργασιών του host system. Τα jails επεκτείνουν αυτό το μοντέλο, με την εικονικοποίηση όχι μόνο της πρόσβασης στο σύστημα αρχείων, αλλά επίσης των χρηστών, του υποσυστήματος δικτύωσης του πυρήνα του FreeBSD και μερικών ακόμη πραγμάτων. Περισσότερα για τις διαθέσιμες εντολές που μπορούν να χρησιμοποιηθούν για τη ρύθμιση και τον έλεγχο ενός περιβάλλοντος jail μπορείτε να βρείτε στο Λεπτομερής Ρύθμιση και Διαχείριση.

Το Jail έχει τέσσερα κύρια στοιχεία:

- Έναν κατάλογο με δική του δομή - το αρχικό σημείο στο οποίο εισέρχεται ένα jail. Από τη στιγμή που μια διεργασία βρίσκεται μέσα σε ένα jail, δεν επιτρέπεται να βγει έξω από τον κατάλογο αυτό. Τα προβλήματα που ταλαιπωρούσαν τον σχεδιασμό του chroot(2) δεν επηρεάζουν τα jails του FreeBSD.
- Ένα hostname (όνομα συστήματος) - το hostname το οποίο θα χρησιμοποιηθεί μέσα στο jail. Τα jails χρησιμοποιούνται κυρίως για την εξυπηρέτηση δικτυακών υπηρεσιών, επομένως η ύπαρξη ενός χαρακτηριστικού hostname που να περιγράφει ταυτόχρονα και τη χρήση του, μπορεί να βοηθήσει αρκετά τον διαχειριστή συστήματος.
- Μια διεύθυνση IP - αυτή η διεύθυνση αντιστοιχεί σε ένα jail και δεν μπορεί να αλλάξει κατά τη διάρκεια της ζωής του. Η διεύθυνση IP ενός jail είναι συνήθως μία διεύθυνση τύπου alias για μια ήδη υπάρχουσα διεπαφή δικτύου (network interface), αλλά κάτι τέτοιο δεν είναι απαραίτητο.
- Μία εντολή - η διαδρομή προς ένα εκτελέσιμο το οποίο θα εκτελείται μέσα στο jail. Η διαδρομή αυτή είναι σχετική ως προς τον γονικό κατάλογο του περιβάλλοντος του jail, και μπορεί να διαφέρει πολύ από jail σε jail ανάλογα με το συγκεκριμένο περιβάλλον.

Εκτός αυτών, τα jails μπορούν να έχουν τις δικές τους ομάδες χρηστών και τον δικό τους χρήστη `root`. Φυσικά, ο έλεγχος που έχει ο χρήστης `root` του jail, περιορίζεται μέσα στο περιβάλλον του jail, και από την οπτική γωνία του host system, ο χρήστης αυτός δεν είναι παντοδύναμος. Επιπλέον, ο χρήστης `root` του jail, δεν μπορεί να εκτελέσει κρίσιμες εργασίες στο σύστημα έξω από το περιβάλλον του jail(8). Περισσότερες πληροφορίες σχετικά με τις δυνατότητες και τους περιορισμούς του `root` θα βρείτε στο Λεπτομερής Ρύθμιση και Διαχείριση.

36.4. Δημιουργώντας και Ελέγχοντας Jails

Μερικοί διαχειριστές συστημάτων κατηγοριοποιούν τα jails σε δύο ενότητες: τα "complete (πλήρη)" jails, τα οποία μιμούνται ένα πραγματικό σύστημα FreeBSD, και τα "service" jails, τα οποία χρησιμοποιούνται για μια εφαρμογή ή υπηρεσία, που πιθανόν εκτελείται με ειδικά προνόμια. Αυτός είναι ένας νοητικός διαχωρισμός και δεν επιδρά στη διαδικασία δημιουργίας ενός jail. Η σελίδα manual του jail(8) περιέχει κατατοπιστικές πληροφορίες για τη διαδικασία δημιουργίας ενός jail:

```
# setenv D /here/is/the/jail
# mkdir -p $D ①
# cd /usr/src
# make buildworld ②
# make installworld DESTDIR=$D ③
# make distribution DESTDIR=$D ④
```

```
# mount -t devfs devfs $D/dev ⑤
```

① Ο καλύτερος τρόπος για να ξεκινήσετε είναι με την επιλογή μιας θέσης (διαδρομής) για το jail σας. Εκεί θα βρίσκονται αποθηκευμένα τα αρχεία του jail όσο αφορά το σύστημα σας. Μια καλή ιδέα είναι το /usr/jail/jailname, όπου *jailname* το hostname με το οποίο θα αναγνωρίζεται το jail. Το σύστημα αρχείων /usr/ έχει συνήθως αρκετό χώρο για το σύστημα αρχείων του jail, το οποίο, για ένα "complete" jail είναι ουσιαστικά ένας κλώνος κάθε αρχείου του βασικού συστήματος μια προεπιλεγμένης εγκατάστασης του FreeBSD.

② Το βήμα αυτό δεν απαιτείται αν έχετε μεταγλωττίσει στο παρελθόν το βασικό σύστημα χρησιμοποιώντας την εντολή `make world` ή `make buildworld`. Μπορείτε απλώς να εγκαταστήσετε το υπάρχον σύστημα σας στο νέο jail.

③ Η εντολή αυτή θα εμπλουτίσει τον κατάλογο που επιλέξατε για το jail με όλα τα απαραίτητα αρχεία, βιβλιοθήκες, σελίδες βοήθειας κλπ.

④ Το `distribution` target του make εγκαθιστά όλα τα αρχεία ρυθμίσεων που απαιτούνται. Με απλά λόγια, εγκαθιστά κάθε αρχείο από το /usr/src/etc/ στον κατάλογο /etc του περιβάλλοντος jail: $D/etc/.

⑤ Δε χρειάζεται να προσαρτήσετε το devfs(8) στο περιβάλλον του jail. Από την άλλη όμως, όλες, ή σχεδόν όλες οι εφαρμογές χρειάζονται πρόσβαση σε τουλάχιστον μία συσκευή, αναλόγως με τον σκοπό της εφαρμογής. Είναι πολύ σημαντικό να ελέγχεται η πρόσβαση στις συσκευές μέσα σε ένα jail, καθώς λανθασμένες ρυθμίσεις μπορεί να επιτρέψουν σε κάποιον εισβολέα να κάνει "άσχημα παιχνίδια" μέσα στο jail. Ο έλεγχος του devfs(8) γίνεται μέσω ενός συνόλου κανόνων οι οποίοι περιγράφονται στις σελίδες manual του devfs(8) και του devfs.conf(5).

Από την στιγμή που έχει εγκατασταθεί ένα jail, μπορεί να εκκινηθεί με τη χρήση της εντολής jail(8). Η jail(8) δέχεται τέσσερις υποχρεωτικές παραμέτρους οι οποίες περιγράφονται στο Τι Είναι Ένα Jail. Μπορείτε να δώσετε και άλλες παραμέτρους, π.χ., για να εκτελέσετε μια διεργασία στο περιβάλλον του jail με τις άδειες ενός συγκεκριμένου χρήστη. Η παράμετρος `command` εξαρτάται από τον τύπο του jail. Για ένα *εικονικό σύστημα*, το /etc/rc είναι μια καλή επιλογή, μια και στην ουσία θα κλωνοποιήσει την διαδικασία εκκίνησης ενός πραγματικού συστήματος FreeBSD. Για ένα *service* jail, η παράμετρος εξαρτάται από την υπηρεσία ή την εφαρμογή που θα τρέχει μέσα στο jail.

Τα jails συνήθως ξεκινούν κατά την εκκίνηση και ο μηχανισμός rc του FreeBSD παρέχει έναν εύκολο τρόπο για να γίνει κάτι τέτοιο.

1. Η λίστα με τα jails που θέλετε να ξεκινάνε κατά την εκκίνηση θα πρέπει να προστεθούν στο αρχείο rc.conf(5):

```
jail_enable="YES"   # Set to NO to disable starting of any jails
jail_list="www"     # Space separated list of names of jails
```

Το όνομα που έχει κάθε jail στη λίστα `jail_list` επιτρέπεται να περιέχει μόνο αλφαριθμητικούς χαρακτήρες.

2. Για κάθε jail που υπάρχει στο `jail_list`, θα πρέπει να προστεθεί μια ομάδα από ρυθμίσεις στο rc.conf(5), οι οποίες θα το περιγράφουν:

```
jail_www_rootdir="/usr/jail/www"     # jail's root directory
jail_www_hostname="www.example.org"  # jail's hostname
jail_www_ip="192.168.0.10"           # jail's IP address
jail_www_devfs_enable="YES"          # mount devfs in the jail
jail_www_devfs_ruleset="www_ruleset" # devfs ruleset to apply to jail
```

Η προεπιλεγμένη εκκίνηση του jail μέσω του rc.conf(5), θα ξεκινήσει το script του jail /etc/rc, το οποίο υποθέτει ότι το jail είναι ένα ολοκληρωμένο εικονικό σύστημα. Για service jails, η προεπιλεγμένη εκκίνηση πρέπει να αλλάξει, ορίζοντας κατάλληλα την επιλογή `jail jailnameexec_start`.

Για πλήρη λίστα των διαθέσιμων επιλογών, δείτε το rc.conf(5).

Το script /etc/rc.d/jail μπορεί να χρησιμοποιηθεί για να ξεκινήσει ή να σταματήσει κάποιο jail χειροκίνητα. Πρέπει όμως να υπάρχει η αντίστοιχη καταχώρηση στο rc.conf:

```
# /etc/rc.d/jail start www
# /etc/rc.d/jail stop www
```

Για την ώρα δεν υπάρχει κάποιος απόλυτα σωστός τρόπος για να τερματίσετε κάποιο jail(8). Αυτό συμβαίνει, διότι οι εντολές που χρησιμοποιούνται συνήθως για να τερματίσουν με ασφάλεια ένα σύστημα, δεν μπορούν να χρησιμοποιηθούν μέσα στο περιβάλλον ενός jail. Ο καλύτερος τρόπος για να τερματίσετε ένα jail είναι με την εκτέλεση της ακόλουθης εντολής μέσα από το ίδιο το jail ή με χρήση του βοηθητικού προγράμματος jexec(8) έξω από αυτό:

```
# sh /etc/rc.shutdown
```

Περισσότερες πληροφορίες σχετικά με αυτή τη διαδικασία μπορείτε να βρείτε στη σελίδα βοηθείας του jail(8)

36.5. Λεπτομερής Ρύθμιση και Διαχείριση

Υπάρχουν αρκετές επιλογές που μπορούν να εφαρμοστούν σε ένα jail, καθώς και διάφοροι τρόποι για να συνδυαστεί ένα σύστημα FreeBSD με jails προκειμένου να παράγουν εφαρμογές υψηλότερου επιπέδου. Η ενότητα αυτή παρουσιάζει:

- Μερικές από τις διαθέσιμες επιλογές για την ρύθμιση της συμπεριφοράς και των περιορισμών ασφαλείας που υλοποιούνται από την εγκατάσταση ενός jail.
- Μερικές εφαρμογές υψηλού επιπέδου για τη διαχείριση jails, οι οποίες είναι διαθέσιμες μέσω της συλλογής των Ports του FreeBSD και μπορούν να χρησιμοποιηθούν στην υλοποίηση ολοκληρωμένων λύσεων με τη χρήση jails.

36.5.1. Εργαλεία Συστήματος του FreeBSD για τη Ρύθμιση Jails

Λεπτομερής ρύθμιση ενός jail γίνεται κατά κύριο λόγο μέσω των μεταβλητών του sysctl(8). Υπάρχει

ένα ειδικό subtree του sysctl το οποίο αποτελεί τη βάση για την οργάνωση όλων των σχετικών επιλογών: πρόκειται για την ιεραρχία επιλογών πυρήνα `security.jail.*`. Παρακάτω θα βρείτε μια λίστα με τα κύρια sysctl που σχετίζονται με κάποιο jail καθώς και τις προεπιλεγμένες τιμές τους. Τα ονόματα μάλλον εξηγούν από μόνα τους την αντίστοιχη λειτουργία, αλλά για περισσότερες πληροφορίες μπορείτε να δείτε τις σελίδες βοήθειας των jail(8) και sysctl(8).

- `security.jail.set_hostname_allowed: 1`
- `security.jail.socket_unixiproute_only: 1`
- `security.jail.sysvipc_allowed: 0`
- `security.jail.enforce_statfs: 2`
- `security.jail.allow_raw_sockets: 0`
- `security.jail.chflags_allowed: 0`
- `security.jail.jailed: 0`

Οι μεταβλητές αυτές μπορούν να χρησιμοποιηθούν από τον διαχειριστή του *host system* προκειμένου να προσθέσει ή να αφαιρέσει περιορισμούς οι οποίοι υπάρχουν αρχικά στον χρήστη `root`. Υπάρχουν όμως και κάποιοι περιορισμοί οι οποίοι δεν μπορούν να αφαιρεθούν. Ο χρήστης `root` δεν επιτρέπεται να προσαρτά ή να απο-προσαρτά συστήματα αρχείων μέσα από ένα jail(8). Ο `root` μέσα σε ένα jail δεν επιτρέπεται να φορτώσει ή να αποφορτώσει τους κανόνες (rulesets) του devfs(8), το firewall, και διάφορες άλλες εργασίες διαχείρισης οι οποίες χρειάζονται τροποποίηση των δεδομένων του πυρήνα, όπως για παράδειγμα ο ορισμός του `securelevel` του πυρήνα.

Το βασικό σύστημα του FreeBSD περιέχει τα βασικά εργαλεία για τη προβολή πληροφοριών σχετικά με τα ενεργά jails, και επίσης για την ανάθεση συγκεκριμένων εντολών διαχείρισης σε κάποιο jail. Οι εντολές jls(8) και jexec(8) αποτελούν μέρος του βασικού συστήματος του FreeBSD, και μπορούν να χρησιμοποιηθούν για να τις παρακάτω απλές εργασίες:

- Προβολή λίστας των ενεργών jails και τον αντίστοιχων χαρακτηριστικών τους - jail identifier (JID), διεύθυνση IP, hostname και path.
- Προσκόλληση σε κάποιο ενεργό jail, από το host system, και εκτέλεση κάποιας εντολής μέσα στο jail ή εκτέλεση εργασιών διαχείρισης μέσα στο jail. Κάτι τέτοιο είναι ιδιαίτερα χρήσιμο όταν ο χρήστης `root` επιθυμεί να τερματίσει με ασφάλεια κάποιο jail. Μπορεί επίσης να χρησιμοποιηθεί η εντολή jexec(8) για την εκτέλεση κάποιου shell μέσα στο jail προκειμένου να εκτελεστούν εργασίες διαχείρισης, για παράδειγμα:

  ```
  # jexec 1 tcsh
  ```

36.5.2. Εργαλεία Διαχείρισης Υψηλού Επιπέδου στη Συλλογή Ports του FreeBSD

Ανάμεσα στις διάφορες εφαρμογές τρίτων κατασκευαστών για τη διαχείριση των jails, ένα από τα ποιο ολοκληρωμένα και χρήσιμα πακέτα είναι το sysutils/jailutils. Αποτελεί ένα σύνολο μικρών εφαρμογών οι οποίες συνεισφέρουν στη διαχείριση του jail(8). Για περισσότερες πληροφορίες, δείτε στον δικτυακό του τόπο.

36.6. Εφαρμογή των Jails

36.6.1. Service Jails

Η ενότητα αυτή είναι βασισμένη στην ιδέα που παρουσιάστηκε αρχικά από τον Simon L. B. Nielsen <simon@FreeBSD.org> στο http://simon.nitro.dk/service-jails.html, καθώς και σε ένα ανανεωμένο άρθρο του Ken Tom locals@gmail.com. Στην ενότητα αυτή θα σας δείξουμε πως να στήσετε ένα σύστημα FreeBSD το οποίο να διαθέτει ένα επιπλέον επίπεδο ασφάλειας, με τη χρήση του jail(8). Υποθέτουμε ότι το σύστημα τρέχει τουλάχιστον RELENG_6_0 και ότι έχετε κατανοήσει όλες τις προηγούμενες πληροφορίες του κεφαλαίου.

36.6.1.1. Σχεδιασμός

Ένα από τα σημαντικότερα προβλήματα με τα jails είναι η διαχείριση της διαδικασίας αναβαθμίσεων. Αυτό τείνει να είναι πρόβλημα διότι το κάθε jail πρέπει να δημιουργηθεί από την αρχή σε κάθε αναβάθμιση. Συνήθως δεν είναι πρόβλημα αν έχετε ένα μόνο jail, μια και πρόκειται για σχετικά απλή διαδικασία, αλλά γίνεται κουραστική και χρονοβόρα αν έχετε πολλά jails.

Οι παρακάτω ρυθμίσεις προϋποθέτουν εμπειρία με το FreeBSD και τη χρήση των διάφορων χαρακτηριστικών του. Εάν τα παρακάτω βήματα σας φαίνονται πολύ περίπλοκα, είναι καλύτερα να ρίξετε μια ματιά σε κάτι ποιο απλό όπως το sysutils/ezjail, το οποίο παρέχει έναν ευκολότερο τρόπο διαχείρισης των jails του FreeBSD και δεν είναι τόσο εξειδικευμένο όσο οι παρακάτω ρυθμίσεις.

Η ιδέα αυτή έχει παρουσιαστεί για να λύσει τέτοιου είδους προβλήματα, με την βοήθεια της κοινής χρήσης όσο το δυνατόν περισσότερων αρχείων μεταξύ των jails, με έναν ασφαλή όμως τρόπο - χρησιμοποιώντας προσαρτήσεις τύπου mount_nullfs(8) και μόνο για ανάγνωση (read only) έτσι ώστε η αναβάθμιση να είναι ευκολότερη, και η χρήση μεμονωμένων jails για κάθε υπηρεσία να καθίσταται επιθυμητή. Επιπλέον, παρέχει έναν απλό τρόπο για να προσθέσετε και να αφαιρέσετε jails όπως επίσης και να τα αναβαθμίσετε.

Παραδείγματα υπηρεσιών τέτοιου τύπου: ένας HTTP server, ένας DNS server, ένας SMTP server, κλπ.

Οι στόχοι των παρακάτω ρυθμίσεων είναι:

- Δημιουργία απλών και κατανοητών jails. Αυτό σημαίνει ότι *δεν* θα τρέξουμε ένα πλήρες installworld σε κάθε jail.
- Εύκολη προσθήκη και διαγραφή jails.
- Εύκολη αναβάθμιση υπαρχόντων jails.
- Δυνατότητα δημιουργίας προσαρμοσμένου τμήματος του FreeBSD.
- Όσο περισσότερη ασφάλεια είναι δυνατόν, με ελαχιστοποίηση της πιθανότητας κακόβουλης χρήσης.
- Εξοικονόμηση χώρου και inodes.

Όπως έχουμε ήδη πει, ο σχεδιασμός αυτός εξαρτάται ιδιαίτερα από την ύπαρξη ενός αρχικού

template στο οποίο δεν επιτρέπεται η εγγραφή δεδομένων (γνωστό ως nullfs) και το οποίο πρέπει να έχει προσαρτηθεί σε κάθε jail, όπως επίσης και στην ύπαρξη για κάθε jail μιας συσκευής που να επιτρέπει τόσο την ανάγνωση όσο και την εγγραφή. Μια τέτοια συσκευή μπορεί να είναι κάποιος ξεχωριστός φυσικός δίσκος, μια κατάτμηση, ή κάποια συσκευή vnode md(4). Στο παρακάτω παράδειγμα, θα χρησιμοποιήσουμε προσαρτήσεις τύπου nullfs στις οποίες θα επιτρέπεται εγγραφή και ανάγνωση.

Η δομή του συστήματος αρχείων περιγράφεται στην παρακάτω λίστα:

- Κάθε jail θα προσαρτάται κάτω από τον κατάλογο /home/j.
- Το /home/j/mroot είναι το template για το κάθε jail και η κατάτμηση μόνο ανάγνωσης για όλα τα jails.
- Θα δημιουργηθεί ένας κενός κατάλογος για κάθε jail κάτω από τον κατάλογο /home/j.
- Κάθε jail θα έχει έναν κατάλογο /s, ο οποίος θα είναι σύνδεσμος προς το εγγράψιμο μέρος του συστήματος.
- Κάθε jail θα έχει το δικό εγγράψιμο μέρος το οποίο θα βασίζεται στο /home/j/skel.
- Κάθε jailspace (το εγγράψιμο μέρος κάθε jail) θα πρέπει να δημιουργηθεί στον κατάλογο /home/js.

Όλα αυτά προϋποθέτουν ότι τα jails βρίσκονται κάτω από τον κατάλογο /home. Αυτό βέβαια μπορεί να αλλάξει σε οτιδήποτε εσείς θέλετε, αλλά θα επηρεάσει όλα τα παρακάτω παραδείγματα.

36.6.1.2. Δημιουργώντας το Template

Η ενότητα αυτή θα περιγράψει τα βήματα που χρειάζονται προκειμένου να δημιουργήσετε το πρωταρχικό template το οποίο θα περιέχει το τμήμα των jails που είναι μόνο για ανάγνωση.

Είναι πάντοτε καλή ιδέα να αναβαθμίζετε το FreeBSD στη τελευταία έκδοση -RELEASE. Για το σκοπό αυτό, διαβάστε το αντίστοιχο κεφάλαιο στο Εγχειρίδιο. Στη περίπτωση που η αναβάθμιση δεν είναι εφικτή, θα χρειαστείτε buildworld για να μπορέσετε να συνεχίσετε. Επιπλέον θα χρειαστείτε το πακέτο sysutils/cpdup. Θα χρησιμοποιήσουμε το βοηθητικό πρόγραμμα portsnap(8) για να κατεβάσουμε τη συλλογή των Ports. Για τους νεο-εισερχόμενους, συνίσταται η ανάγνωση του κεφαλαίου για το Portsnap στο Εγχειρίδιο του FreeBSD.

1. Αρχικά, δημιουργήστε μια δομή καταλόγων για το σύστημα αρχείων το οποίο θα είναι μόνο για ανάγνωση, και το οποίο θα περιέχει τα εκτελέσιμα (binaries) του FreeBSD για τα jails. Στη συνέχεια πηγαίνετε στον κατάλογο όπου βρίσκονται τα αρχεία πηγαίου κώδικα (source tree) του FreeBSD και εγκαταστήστε τα αντίστοιχα αρχεία στο jail template:

```
# mkdir /home/j /home/j/mroot
# cd /usr/src
# make installworld DESTDIR=/home/j/mroot
```

2. Επόμενο βήμα είναι να προετοιμάσετε τη συλλογή των Ports του FreeBSD για τα jails όπως επίσης και ένα FreeBSD source tree, το οποίο θα χρειαστεί για το mergemaster:

```
# cd /home/j/mroot
# mkdir usr/ports
# portsnap -p /home/j/mroot/usr/ports fetch extract
# cpdup /usr/src /home/j/mroot/usr/src
```

3. Δημιουργήστε το σκελετό για το τμήμα του συστήματος όπου προορίζεται για ανάγνωση και εγγραφή:

```
# mkdir /home/j/skel /home/j/skel/home /home/j/skel/usr-X11R6
/home/j/skel/distfiles
# mv etc /home/j/skel
# mv usr/local /home/j/skel/usr-local
# mv tmp /home/j/skel
# mv var /home/j/skel
# mv root /home/j/skel
```

4. Χρησιμοποιήστε το mergemaster για να εγκαταστήσετε τα αρχεία ρυθμίσεων που λείπουν. Στη συνέχεια διαγράψτε όλους τους έξτρα καταλόγους που δημιουργεί το mergemaster:

```
# mergemaster -t /home/j/skel/var/tmp/temproot -D /home/j/skel -i
# cd /home/j/skel
# rm -R bin boot lib libexec mnt proc rescue sbin sys usr dev
```

5. Τώρα, δημιουργήστε συνδέσμους από το σύστημα αρχείων στο οποίο επιτρέπεται η εγγραφή, προς το σύστημα αρχείων που είναι μόνο για ανάγνωση. Βεβαιωθείτε ότι οι σύνδεσμοι έχουν δημιουργηθεί στις σωστές θέσεις s/. Η ύπαρξη πραγματικών καταλόγων ή η δημιουργία καταλόγων σε λάθος θέσεις θα οδηγήσουν την εγκατάσταση σε αποτυχία.

```
# cd /home/j/mroot
# mkdir s
# ln -s s/etc etc
# ln -s s/home home
# ln -s s/root root
# ln -s ../s/usr-local usr/local
# ln -s ../s/usr-X11R6 usr/X11R6
# ln -s ../../s/distfiles usr/ports/distfiles
# ln -s s/tmp tmp
# ln -s s/var var
```

6. Σαν τελευταίο βήμα, δημιουργήστε ένα γενικό αρχείο /home/j/skel/etc/make.conf με τα παρακάτω δεδομένα:

```
WRKDIRPREFIX?=  /s/portbuild
```

Έχοντας ορίσει το WRKDIRPREFIX με αυτόν τον τρόπο, θα μπορείτε να μεταγλωττίσετε ports του FreeBSD μέσα σε κάθε jail. Θυμηθείτε ότι ο κατάλογος των ports είναι μέρος του συστήματος αρχείων που έχει προσαρτηθεί μόνο για ανάγνωση. Η προσαρμοσμένη διαδρομή για το WRKDIRPREFIX επιτρέπει την μεταγλώττιση των ports στο εγγράψιμο μέρος του κάθε jail.

36.6.1.3. Δημιουργώντας Jails

Τώρα που έχουμε ένα ολοκληρωμένο FreeBSD jail template, μπορούμε να εγκαταστήσουμε και να ρυθμίσουμε τα jails στο /etc/rc.conf. Το παράδειγμα αυτό δείχνει τη δημιουργία τριών jails: "NS", "MAIL" και "WWW".

1. Εισάγετε τις παρακάτω γραμμές στο αρχείο /etc/fstab, ώστε το μόνο για ανάγνωση template για τα jails και ο εγγράψιμος χώρος να είναι διαθέσιμα στα αντίστοιχα jails:

```
/home/j/mroot   /home/j/ns     nullfs  ro  0   0
/home/j/mroot   /home/j/mail   nullfs  ro  0   0
/home/j/mroot   /home/j/www    nullfs  ro  0   0
/home/js/ns     /home/j/ns/s   nullfs  rw  0   0
/home/js/mail   /home/j/mail/s nullfs  rw  0   0
/home/js/www    /home/j/www/s  nullfs  rw  0   0
```

Οι κατατμήσεις που είναι σημειωμένες με 0 pass number δεν ελέγχονται κατά την εκκίνηση από το fsck(8), ενώ για τις κατατμήσεις με 0 dump number, η dump(8) δεν θα δημιουργεί αντίγραφα ασφαλείας. Προφανώς, δεν θέλουμε το fsck να ελέγχει τις προσαρτήσεις τύπου nullfs, ούτε και το dump να κρατά αντίγραφα από τα μόνο για ανάγνωση nullfs συστήματα αρχείων των jails. Αυτός είναι και ο λόγος που βάλαμε "0 0" στις δύο τελευταίες στήλες κάθε εγγραφής του fstab.

2. Ρυθμίστε τα jails στο /etc/rc.conf:

```
jail_enable="YES"
jail_set_hostname_allow="NO"
jail_list="ns mail www"
jail_ns_hostname="ns.example.org"
jail_ns_ip="192.168.3.17"
jail_ns_rootdir="/home/j/ns"
jail_ns_devfs_enable="YES"
jail_mail_hostname="mail.example.org"
jail_mail_ip="192.168.3.18"
jail_mail_rootdir="/home/j/mail"
jail_mail_devfs_enable="YES"
jail_www_hostname="www.example.org"
jail_www_ip="62.123.43.14"
jail_www_rootdir="/home/j/www"
jail_www_devfs_enable="YES"
```

Ο λόγος για τον οποίο θέτουμε τη μεταβλητή `jailnamerootdir` να δείχνει στο /usr/home αντί για το /home είναι ότι η φυσική διαδρομή για τον κατάλογο /home σε μια τυπική εγκατάσταση του FreeBSD είναι το /usr/home. Η μεταβλητή `jailnamerootdir` *δεν* δεν πρέπει να δείχνει προς διαδρομή που περιλαμβάνει συμβολικό δεσμό, διαφορετικά τα jails θα αρνηθούν να ξεκινήσουν. Χρησιμοποιήστε το βοηθητικό πρόγραμμα realpath(1) για να προσδιορίσετε την τιμή που θα πρέπει να λάβει αυτή η μεταβλητή. Δείτε το FreeBSD-SA-07:01.jail Security Advisory για περισσότερες πληροφορίες.

3. Δημιουργήστε τα απαραίτητα σημεία προσαρτήσεων για το σύστημα αρχείων μόνο ανάγνωσης του κάθε jail:

```
# mkdir /home/j/ns /home/j/mail /home/j/www
```

4. Εγκαταστήστε το εγγράψιμο template μέσα στο κάθε jail. Προσέξτε εδώ τη χρήση του sysutils/cpdup, το οποίο επιβεβαιώνει ότι δημιουργείται το σωστό αντίγραφο του κάθε καταλόγου:

```
# mkdir /home/js
# cpdup /home/j/skel /home/js/ns
# cpdup /home/j/skel /home/js/mail
# cpdup /home/j/skel /home/js/www
```

5. Σε αυτή τη φάση, τα jails έχουν δημιουργηθεί και είναι έτοιμα να ξεκινήσουν. Προσαρτήστε το σωστό σύστημα αρχείων για το κάθε jail, και στη συνέχεια εκκινήστε τα, χρησιμοποιώντας το script /etc/rc.d/jail:

```
# mount -a
# /etc/rc.d/jail start
```

Τα jails θα πρέπει τώρα να εκτελούνται κανονικά. Για να ελέγξετε αν έχουν ξεκινήσει σωστά, χρησιμοποιείστε την εντολή jls(8). Θα πρέπει να δείτε κάτι αντίστοιχο με το παρακάτω:

```
# jls
   JID  IP Address      Hostname                      Path
     3  192.168.3.17    ns.example.org                /home/j/ns
     2  192.168.3.18    mail.example.org              /home/j/mail
     1  62.123.43.14    www.example.org               /home/j/www
```

Σε αυτό το σημείο, θα πρέπει να μπορείτε να συνδεθείτε σε κάθε jail, να προσθέσετε νέους χρήστες ή να ρυθμίσετε υπηρεσίες. Η στήλη `JID` δηλώνει το χαρακτηριστικό αναγνωριστικό αριθμό κάθε ενεργού jail. Χρησιμοποιήστε την παρακάτω εντολή προκειμένου να εκτελέσετε εργασίες διαχείρισης του jail, με `JID` 3:

```
# jexec 3 tcsh
```

36.6.1.4. Αναβάθμιση

Κάποια στιγμή, θα χρειαστεί να αναβαθμίσετε το σύστημά σας σε μια νέα έκδοση του FreeBSD, είτε για λόγους ασφάλειας, είτε γιατί υπάρχουν νέες δυνατότητες στην νεώτερη έκδοση οι οποίες είναι χρήσιμες για τα jails που ήδη έχετε. Ο τρόπος που χρησιμοποιήσαμε για την δημιουργία των jails, επιτρέπει την εύκολη αναβάθμιση τους. Επιπλέον, ελαχιστοποιεί το χρόνο διακοπής της λειτουργίας τους, μια και θα χρειαστεί να τα σταματήσετε μόνο κατά τα λίγα τελευταία λεπτά. Επίσης, παρέχει έναν τρόπο να επιστρέψετε σε παλαιότερες εκδόσεις εάν προκύψουν οποιαδήποτε σφάλματα.

1. Το πρώτο βήμα είναι να αναβαθμίσετε το σύστημα στο οποίο φιλοξενούνται τα jails, με το συνήθη τρόπο. Στη συνέχεια δημιουργήστε ένα νέο προσωρινό template κατάλογο, μόνο για ανάγνωση, στο /home/j/mroot2.

   ```
   # mkdir /home/j/mroot2
   # cd /usr/src
   # make installworld DESTDIR=/home/j/mroot2
   # cd /home/j/mroot2
   # cpdup /usr/src usr/src
   # mkdir s
   ```

   Το `installworld` δημιουργεί μερικούς καταλόγους που δε χρειάζονται, και θα πρέπει να διαγραφούν:

   ```
   # chflags -R 0 var
   # rm -R etc var root usr/local tmp
   ```

2. Δημιουργήστε ξανά τους συνδέσμους για το σύστημα αρχείων ανάγνωσης - εγγραφής:

   ```
   # ln -s s/etc etc
   # ln -s s/root root
   # ln -s s/home home
   # ln -s ../s/usr-local usr/local
   # ln -s ../s/usr-X11R6 usr/X11R6
   # ln -s s/tmp tmp
   # ln -s s/var var
   ```

3. Τώρα είναι η σωστή στιγμή για να σταματήσετε τα jails:

   ```
   # /etc/rc.d/jail stop
   ```

4. Αποπροσαρτήστε τα αρχικά συστήματα αρχείων:

```
# umount /home/j/ns/s
# umount /home/j/ns
# umount /home/j/mail/s
# umount /home/j/mail
# umount /home/j/www/s
# umount /home/j/www
```

Τα συστήματα αρχείων ανάγνωσης - εγγραφής είναι προσαρτημένα στο σύστημα αρχείων μόνο ανάγνωσης (/s) και πρέπει να είναι τα πρώτα που θα αποπροσαρτηθούν.

5. Μετακινήστε τον παλιό μόνο για ανάγνωση κατάλογο, και αντικαταστήστε τον με τον καινούργιο. Ο παλιός θα παραμείνει ως αντίγραφο ασφαλείας του παλιού συστήματος σε περίπτωση προβλήματος. Ο τρόπος ονομασίας που ακολουθήσαμε εδώ αντιστοιχεί στη χρονική στιγμή δημιουργίας του νέου συστήματος αρχείων μόνο ανάγνωσης. Μετακινήστε την αρχική συλλογή των Ports του FreeBSD στο νέο σύστημα, αρχείων προκειμένου να εξοικονομήσετε χώρο και inodes:

```
# cd /home/j
# mv mroot mroot.20060601
# mv mroot2 mroot
# mv mroot.20060601/usr/ports mroot/usr
```

6. Σε αυτό το σημείο το μόνο για ανάγνωση template είναι έτοιμο, οπότε το μόνο που απομένει είναι να προσαρτήσετε ξανά τα συστήματα αρχείων και να ξεκινήσετε τα jails:

```
# mount -a
# /etc/rc.d/jail start
```

Χρησιμοποιείτε την εντολή jls(8) για να ελέγξετε εάν τα jails ξεκίνησαν σωστά. Μην ξεχάσετε να εκτελέσετε το mergemaster για το κάθε jail. Θα χρειαστεί να αναβαθμίσετε τόσο τα αρχεία ρυθμίσεων, όσο και τα rc.d scripts.

Chapter 37. Υποχρεωτικός Έλεγχος Πρόσβασης

37.1. Σύνοψη

Το FreeBSD 5.X εισήγαγε νέες επεκτάσεις ασφαλείας από το TrustedBSD project, που βασίζονται στο προσχέδιο POSIX®.1e. Δύο από τους πιο σημαντικούς νέους μηχανισμούς ασφαλείας, είναι οι Λίστες Ελέγχου Πρόσβασης (Access Control Lists, ACLs) στο σύστημα αρχείων και ο Υποχρεωτικός Έλεγχος Πρόσβασης (Mandatory Access Control, MAC). Ο Υποχρεωτικός Έλεγχος Πρόσβασης δίνει την δυνατότητας φόρτωσης αρθρωμάτων (modules) ελέγχου τα οποία υλοποιούν νέες πολιτικές ασφαλείας. Μερικά παρέχουν προστασία σε ένα στενό υποσύνολο του συστήματος, ενδυναμώνοντας την ασφάλεια μιας συγκεκριμένης υπηρεσίας. Άλλα παρέχουν συνοπτική ασφάλεια προς όλες τις υπηρεσίες και το σύστημα. Ο έλεγχος ονομάζεται υποχρεωτικός από το γεγονός ότι η επιβολή γίνεται από τους διαχειριστές και το σύστημα, και δεν αφήνεται στη διακριτική ευχέρεια των χρηστών όπως γίνεται με το διακριτικό έλεγχο πρόσβασης (Discretionary Access Control, DAC, τις τυποποιημένες άδειες αρχείων και IPC του System V στο FreeBSD).

Το κεφάλαιο αυτό εστιάζει στο πλαίσιο του Υποχρεωτικού Ελέγχου Πρόσβασης (MAC Framework), και σε ένα σύνολο πρόσθετων αρθρωμάτων για πολιτικές ασφάλειας, που ενεργοποιούν διάφορους μηχανισμούς ασφάλειας.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τι MAC αρθρώματα πολιτικών ασφαλείας περιλαμβάνονται αυτή τη στιγμή στο FreeBSD και τους σχετικούς μηχανισμούς τους.
- Τι υλοποιούν τα MAC αρθρώματα πολιτικών ασφαλείας καθώς και τη διαφορά μεταξύ μια χαρακτηρισμένης (labeled) και μη χαρακτηρισμένης (non-labeled) πολιτικής.
- Πως να ρυθμίσετε αποδοτικά ένα σύστημα για χρήση του πλαισίου λειτουργιών MAC.
- Πως να ρυθμίσετε τα διαφορετικά αρθρώματα πολιτικών ασφάλειας τα οποία περιλαμβάνονται στο πλαίσιο λειτουργιών MAC .
- Πως να υλοποιήσετε ένα πιο ασφαλές περιβάλλον, χρησιμοποιώντας το πλαίσιο λειτουργιών MAC και τα παραδείγματα που φαίνονται.
- Πως να ελέγξετε τη ρύθμιση του MAC για να εξασφαλίσετε ότι έχει γίνει σωστή υλοποίηση του πλαισίου λειτουργιών.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε τις βασικές έννοιες του UNIX® και του FreeBSD. (Βασικές Έννοιες στο UNIX®).
- Να είστε εξοικειωμένος με τις βασικές έννοιες της ρύθμισης και μεταγλώττισης του πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να έχετε κάποια εξοικείωση με την ασφάλεια και πως αυτή σχετίζεται με το FreeBSD (Ασφάλεια).

Η κακή χρήση των πληροφοριών που παρέχονται εδώ μπορεί να προκαλέσει απώλεια πρόσβασης στο σύστημα, εκνευρισμό στους χρήστες ή αδυναμία

> πρόσβασης στις υπηρεσίες που παρέχονται από το X11. Ακόμα πιο σημαντικό είναι ότι δεν πρέπει να βασίζεστε στο MAC για την πλήρη ασφάλιση ενός συστήματος. Το πλαίσιο λειτουργιών MAC παρέχει απλώς επιπλέον υποστήριξη σε μια υπάρχουσα πολιτική ασφαλείας. Χωρίς σωστές πρακτικές και τακτικούς ελέγχους ασφαλείας, το σύστημα δεν θα είναι ποτέ απόλυτα ασφαλές.
>
> Θα πρέπει επίσης να σημειωθεί ότι τα παραδείγματα που περιέχονται σε αυτό το κεφάλαιο είναι ακριβώς και μόνο αυτό: παραδείγματα. Δεν συνίσταται να χρησιμοποιηθούν ακριβώς αυτές οι ρυθμίσεις σε ένα σύστημα παραγωγής. Η υλοποίηση των διάφορων αρθρωμάτων πολιτικών ασφαλείας απαιτεί αρκετή σκέψη και δοκιμές. Αν δεν κατανοείτε την ακριβή λειτουργία τους, μπορεί να βρεθείτε στη θέση να ελέγχετε ξανά ολόκληρο το σύστημα και να αλλάζετε ρυθμίσεις σε πολλά αρχεία και καταλόγους.

37.1.1. Τι δεν Περιλαμβάνεται στο Κεφάλαιο

Το κεφάλαιο αυτό καλύπτει μια ευρεία περιοχή προβλημάτων ασφαλείας που σχετίζονται με το πλαίσιο λειτουργιών MAC. Δεν θα καλυφθεί η ανάπτυξη νέων αρθρωμάτων πολιτικών ασφαλείας MAC. Ένας αριθμός από αρθρώματα που περιλαμβάνονται στο πλαίσιο MAC, έχουν ειδικά χαρακτηριστικά που παρέχονται τόσο για δοκιμές όσο και για ανάπτυξη νέων αρθρωμάτων. Αυτά περιλαμβάνουν τα mac_test(4), mac_stub(4) και mac_none(4). Για περισσότερες πληροφορίες σχετικά με αυτά τα αρθρώματα και τους διάφορους μηχανισμούς που παρέχουν, παρακαλούμε ανατρέξτε στις αντίστοιχες σελίδες manual.

37.2. Key Terms in this Chapter

Before reading this chapter, a few key terms must be explained. This will hopefully clear up any confusion that may occur and avoid the abrupt introduction of new terms and information.

- *compartment*: A compartment is a set of programs and data to be partitioned or separated, where users are given explicit access to specific components of a system. Also, a compartment represents a grouping, such as a work group, department, project, or topic. Using compartments, it is possible to implement a need-to-know security policy.
- *high water mark*: A high water mark policy is one which permits the raising of security levels for the purpose of accessing higher level information. In most cases, the original level is restored after the process is complete. Currently, the FreeBSD MAC framework does not have a policy for this, but the definition is included for completeness.
- *integrity*: Integrity, as a key concept, is the level of trust which can be placed on data. As the integrity of the data is elevated, so does the ability to trust that data.
- *label*: A label is a security attribute which can be applied to files, directories, or other items in the system. It could be considered a confidentiality stamp; when a label is placed on a file it describes the security properties for that specific file and will only permit access by files, users, resources, etc. with a similar security setting. The meaning and interpretation of label values depends on the policy configuration: while some policies might treat a label as representing the integrity or secrecy of an object, other policies might use labels to hold rules for access.
- *level*: The increased or decreased setting of a security attribute. As the level increases, its

security is considered to elevate as well.

- *low water mark*: A low water mark policy is one which permits lowering of the security levels for the purpose of accessing information which is less secure. In most cases, the original security level of the user is restored after the process is complete. The only security policy module in FreeBSD to use this is mac_lomac(4).
- *multilabel*: The `multilabel` property is a file system option which can be set in single user mode using the tunefs(8) utility, during the boot operation using the fstab(5) file, or during the creation of a new file system. This option will permit an administrator to apply different MAC labels on different objects. This option only applies to security policy modules which support labeling.
- *object*: An object or system object is an entity through which information flows under the direction of a *subject*. This includes directories, files, fields, screens, keyboards, memory, magnetic storage, printers or any other data storage/moving device. Basically, an object is a data container or a system resource; access to an *object* effectively means access to the data.
- *policy*: A collection of rules which defines how objectives are to be achieved. A *policy* usually documents how certain items are to be handled. This chapter will consider the term *policy* in this context as a *security policy*; i.e. a collection of rules which will control the flow of data and information and define whom will have access to that data and information.
- *sensitivity*: Usually used when discussing MLS. A sensitivity level is a term used to describe how important or secret the data should be. As the sensitivity level increases, so does the importance of the secrecy, or confidentiality of the data.
- *single label*: A single label is when the entire file system uses one label to enforce access control over the flow of data. When a file system has this set, which is any time when the `multilabel` option is not set, all files will conform to the same label setting.
- *subject*: a subject is any active entity that causes information to flow between *objects*; e.g. a user, user processor, system process, etc. On FreeBSD, this is almost always a thread acting in a process on behalf of a user.

37.3. Explanation of MAC

With all of these new terms in mind, consider how the MAC framework augments the security of the system as a whole. The various security policy modules provided by the MAC framework could be used to protect the network and file systems, block users from accessing certain ports and sockets, and more. Perhaps the best use of the policy modules is to blend them together, by loading several security policy modules at a time for a multi-layered security environment. In a multi-layered security environment, multiple policy modules are in effect to keep security in check. This is different to a hardening policy, which typically hardens elements of a system that is used only for specific purposes. The only downside is administrative overhead in cases of multiple file system labels, setting network access control user by user, etc.

These downsides are minimal when compared to the lasting effect of the framework; for instance, the ability to pick and choose which policies are required for a specific configuration keeps performance overhead down. The reduction of support for unneeded policies can increase the overall performance of the system as well as offer flexibility of choice. A good implementation would consider the overall security requirements and effectively implement the various security

policy modules offered by the framework.

Thus a system utilizing MAC features should at least guarantee that a user will not be permitted to change security attributes at will; all user utilities, programs and scripts must work within the constraints of the access rules provided by the selected security policy modules; and that total control of the MAC access rules are in the hands of the system administrator.

It is the sole duty of the system administrator to carefully select the correct security policy modules. Some environments may need to limit access control over the network; in these cases, the mac_portacl(4), mac_ifoff(4) and even mac_biba(4) policy modules might make good starting points. In other cases, strict confidentiality of file system objects might be required. Policy modules such as mac_bsdextended(4) and mac_mls(4) exist for this purpose.

Policy decisions could be made based on network configuration. Perhaps only certain users should be permitted access to facilities provided by ssh(1) to access the network or the Internet. The mac_portacl(4) would be the policy module of choice for these situations. But what should be done in the case of file systems? Should all access to certain directories be severed from other groups or specific users? Or should we limit user or utility access to specific files by setting certain objects as classified?

In the file system case, access to objects might be considered confidential to some users, but not to others. For an example, a large development team might be broken off into smaller groups of individuals. Developers in project A might not be permitted to access objects written by developers in project B. Yet they might need to access objects created by developers in project C; that is quite a situation indeed. Using the different security policy modules provided by the MAC framework; users could be divided into these groups and then given access to the appropriate areas without fear of information leakage.

Thus, each security policy module has a unique way of dealing with the overall security of a system. Module selection should be based on a well thought out security policy. In many cases, the overall policy may need to be revised and reimplemented on the system. Understanding the different security policy modules offered by the MAC framework will help administrators choose the best policies for their situations.

The default FreeBSD kernel does not include the option for the MAC framework; thus the following kernel option must be added before trying any of the examples or information in this chapter:

```
options MAC
```

And the kernel will require a rebuild and a reinstall.

While the various manual pages for MAC policy modules state that they may be built into the kernel, it is possible to lock the system out of the network and more. Implementing MAC is much like implementing a firewall, care must be taken to prevent being completely locked out of the system. The ability to revert back to a previous configuration should be considered while the implementation of MAC remotely should be done with extreme caution.

37.4. Understanding MAC Labels

A MAC label is a security attribute which may be applied to subjects and objects throughout the system.

When setting a label, the user must be able to comprehend what it is, exactly, that is being done. The attributes available on an object depend on the policy module loaded, and that policy modules interpret their attributes in different ways. If improperly configured due to lack of comprehension, or the inability to understand the implications, the result will be the unexpected and perhaps, undesired, behavior of the system.

The security label on an object is used as a part of a security access control decision by a policy. With some policies, the label by itself contains all information necessary to make a decision; in other models, the labels may be processed as part of a larger rule set, etc.

For instance, setting the label of `biba/low` on a file will represent a label maintained by the Biba security policy module, with a value of "low".

A few policy modules which support the labeling feature in FreeBSD offer three specific predefined labels. These are the low, high, and equal labels. Although they enforce access control in a different manner with each policy module, you can be sure that the low label will be the lowest setting, the equal label will set the subject or object to be disabled or unaffected, and the high label will enforce the highest setting available in the Biba and MLS policy modules.

Within single label file system environments, only one label may be used on objects. This will enforce one set of access permissions across the entire system and in many environments may be all that is required. There are a few cases where multiple labels may be set on objects or subjects in the file system. For those cases, the `multilabel` option may be passed to tunefs(8).

In the case of Biba and MLS, a numeric label may be set to indicate the precise level of hierarchical control. This numeric level is used to partition or sort information into different groups of say, classification only permitting access to that group or a higher group level.

In most cases the administrator will only be setting up a single label to use throughout the file system.

Hey wait, this is similar to DAC! I thought MAC gave control strictly to the administrator. That statement still holds true, to some extent as `root` is the one in control and who configures the policies so that users are placed in the appropriate categories/access levels. Alas, many policy modules can restrict the `root` user as well. Basic control over objects will then be released to the group, but `root` may revoke or modify the settings at any time. This is the hierarchal/clearance model covered by policies such as Biba and MLS.

37.4.1. Label Configuration

Virtually all aspects of label policy module configuration will be performed using the base system utilities. These commands provide a simple interface for object or subject configuration or the manipulation and verification of the configuration.

All configuration may be done by use of the setfmac(8) and setpmac(8) utilities. The `setfmac`

command is used to set MAC labels on system objects while the `setpmac` command is used to set the labels on system subjects. Observe:

```
# setfmac biba/high test
```

If no errors occurred with the command above, a prompt will be returned. The only time these commands are not quiescent is when an error occurred; similarly to the chmod(1) and chown(8) commands. In some cases this error may be a `Permission denied` and is usually obtained when the label is being set or modified on an object which is restricted. The system administrator may use the following commands to overcome this:

```
# setfmac biba/high test
Permission denied
# setpmac biba/low setfmac biba/high test
# getfmac test
test: biba/high
```

As we see above, `setpmac` can be used to override the policy module's settings by assigning a different label to the invoked process. The `getpmac` utility is usually used with currently running processes, such as sendmail: although it takes a process ID in place of a command the logic is extremely similar. If users attempt to manipulate a file not in their access, subject to the rules of the loaded policy modules, the `Operation not permitted` error will be displayed by the `mac_set_link` function.

37.4.1.1. Common Label Types

For the mac_biba(4), mac_mls(4) and mac_lomac(4) policy modules, the ability to assign simple labels is provided. These take the form of high, equal and low, what follows is a brief description of what these labels provide:

- The `low` label is considered the lowest label setting an object or subject may have. Setting this on objects or subjects will block their access to objects or subjects marked high.
- The `equal` label should only be placed on objects considered to be exempt from the policy.
- The `high` label grants an object or subject the highest possible setting.

With respect to each policy module, each of those settings will instate a different information flow directive. Reading the proper manual pages will further explain the traits of these generic label configurations.

37.4.1.1.1. Advanced Label Configuration

Numeric grade labels are used for `comparison:compartment+compartment`; thus the following:

```
biba/10:2+3+6(5:2+3-20:2+3+4+5+6)
```

May be interpreted as:

"Biba Policy Label"/"Grade 10" :"Compartments 2, 3 and 6": ("grade 5 ...")

In this example, the first grade would be considered the "effective grade" with "effective compartments", the second grade is the low grade and the last one is the high grade. In most configurations these settings will not be used; indeed, they offered for more advanced configurations.

When applied to system objects, they will only have a current grade/compartments as opposed to system subjects as they reflect the range of available rights in the system, and network interfaces, where they are used for access control.

The grade and compartments in a subject and object pair are used to construct a relationship referred to as "dominance", in which a subject dominates an object, the object dominates the subject, neither dominates the other, or both dominate each other. The "both dominate" case occurs when the two labels are equal. Due to the information flow nature of Biba, you have rights to a set of compartments, "need to know", that might correspond to projects, but objects also have a set of compartments. Users may have to subset their rights using `su` or `setpmac` in order to access objects in a compartment from which they are not restricted.

37.4.1.2. Users and Label Settings

Users themselves are required to have labels so that their files and processes may properly interact with the security policy defined on the system. This is configured through the login.conf file by use of login classes. Every policy module that uses labels will implement the user class setting.

An example entry containing every policy module setting is displayed below:

```
default:\
    :welcome=/etc/motd:\
    :setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
    :path=~/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin:\
    :manpath=/usr/shared/man /usr/local/man:\
    :nologin=/usr/sbin/nologin:\
    :cputime=1h30m:\
    :datasize=8M:\
    :vmemoryuse=100M:\
    :stacksize=2M:\
    :memorylocked=4M:\
    :memoryuse=8M:\
    :filesize=8M:\
    :coredumpsize=8M:\
    :openfiles=24:\
    :maxproc=32:\
    :priority=0:\
    :requirehome:\
    :passwordtime=91d:\
    :umask=022:\
    :ignoretime@:\
    :label=partition/13,mls/5,biba/10(5-15),lomac/10[2]:
```

The label option is used to set the user class default label which will be enforced by MAC. Users will never be permitted to modify this value, thus it can be considered not optional in the user case. In a real configuration, however, the administrator will never wish to enable every policy module. It is recommended that the rest of this chapter be reviewed before any of this configuration is implemented.

Users may change their label after the initial login; however, this change is subject constraints of the policy. The example above tells the Biba policy that a process's minimum integrity is 5, its maximum is 15, but the default effective label is 10. The process will run at 10 until it chooses to change label, perhaps due to the user using the setpmac command, which will be constrained by Biba to the range set at login.

In all cases, after a change to login.conf, the login class capability database must be rebuilt using cap_mkdb and this will be reflected throughout every forthcoming example or discussion.

It is useful to note that many sites may have a particularly large number of users requiring several different user classes. In depth planning is required as this may get extremely difficult to manage.

Future versions of FreeBSD will include a new way to deal with mapping users to labels; however, this will not be available until some time after FreeBSD 5.3.

37.4.1.3. Network Interfaces and Label Settings

Labels may also be set on network interfaces to help control the flow of data across the network. In all cases they function in the same way the policies function with respect to objects. Users at high settings in biba, for example, will not be permitted to access network interfaces with a label of low.

The maclabel may be passed to ifconfig when setting the MAC label on network interfaces. For example:

```
# ifconfig bge0 maclabel biba/equal
```

will set the MAC label of biba/equal on the bge(4) interface. When using a setting similar to biba/high(low-high) the entire label should be quoted; otherwise an error will be returned.

Each policy module which supports labeling has a tunable which may be used to disable the MAC label on network interfaces. Setting the label to equal will have a similar effect. Review the output from sysctl, the policy manual pages, or even the information found later in this chapter for those tunables.

37.4.2. Singlelabel or Multilabel?

By default the system will use the singlelabel option. But what does this mean to the administrator? There are several differences which, in their own right, offer pros and cons to the flexibility in the systems security model.

The singlelabel only permits for one label, for instance biba/high to be used for each subject or

object. It provides for lower administration overhead but decreases the flexibility of policies which support labeling. Many administrators may want to use the `multilabel` option in their security policy.

The `multilabel` option will permit each subject or object to have its own independent MAC label in place of the standard `singlelabel` option which will allow only one label throughout the partition. The `multilabel` and `single` label options are only required for the policies which implement the labeling feature, including the Biba, Lomac, MLS and SEBSD policies.

In many cases, the `multilabel` may not need to be set at all. Consider the following situation and security model:

- FreeBSD web-server using the MAC framework and a mix of the various policies.
- This machine only requires one label, `biba/high`, for everything in the system. Here the file system would not require the `multilabel` option as a single label will always be in effect.
- But, this machine will be a web server and should have the web server run at `biba/low` to prevent write up capabilities. The Biba policy and how it works will be discussed later, so if the previous comment was difficult to interpret just continue reading and return. The server could use a separate partition set at `biba/low` for most if not all of its runtime state. Much is lacking from this example, for instance the restrictions on data, configuration and user settings; however, this is just a quick example to prove the aforementioned point.

If any of the non-labeling policies are to be used, then the `multilabel` option would never be required. These include the `seeotheruids`, `portacl` and `partition` policies.

It should also be noted that using `multilabel` with a partition and establishing a security model based on `multilabel` functionality could open the doors for higher administrative overhead as everything in the file system would have a label. This includes directories, files, and even device nodes.

The following command will set `multilabel` on the file systems to have multiple labels. This may only be done in single user mode:

```
# tunefs -l enable /
```

This is not a requirement for the swap file system.

Some users have experienced problems with setting the `multilabel` flag on the root partition. If this is the case, please review the Troubleshooting the MAC Framework of this chapter.

37.5. Planning the Security Configuration

Whenever a new technology is implemented, a planning phase is always a good idea. During the planning stages, an administrator should in general look at the "big picture", trying to keep in view at least the following:

- The implementation requirements;
- The implementation goals;

For MAC installations, these include:

- How to classify information and resources available on the target systems.
- What sorts of information or resources to restrict access to along with the type of restrictions that should be applied.
- Which MAC module or modules will be required to achieve this goal.

It is always possible to reconfigure and change the system resources and security settings, it is quite often very inconvenient to search through the system and fix existing files and user accounts. Planning helps to ensure a trouble-free and efficient trusted system implementation. A trial run of the trusted system, including the configuration, is often vital and definitely beneficial *before* a MAC implementation is used on production systems. The idea of just letting loose on a system with MAC is like setting up for failure.

Different environments may have explicit needs and requirements. Establishing an in depth and complete security profile will decrease the need of changes once the system goes live. As such, the future sections will cover the different modules available to administrators; describe their use and configuration; and in some cases provide insight on what situations they would be most suitable for. For instance, a web server might roll out the mac_biba(4) and mac_bsdextended(4) policies. In other cases, a machine with very few local users, the mac_partition(4) might be a good choice.

37.6. Module Configuration

Every module included with the MAC framework may be either compiled into the kernel as noted above or loaded as a run-time kernel module. The recommended method is to add the module name to the /boot/loader.conf file so that it will load during the initial boot operation.

The following sections will discuss the various MAC modules and cover their features. Implementing them into a specific environment will also be a consideration of this chapter. Some modules support the use of labeling, which is controlling access by enforcing a label such as "this is allowed and this is not". A label configuration file may control how files may be accessed, network communication can be exchanged, and more. The previous section showed how the `multilabel` flag could be set on file systems to enable per-file or per-partition access control.

A single label configuration would enforce only one label across the system, that is why the `tunefs` option is called `multilabel`.

37.6.1. The MAC seeotheruids Module

Module name: mac_seeotheruids.ko

Kernel configuration line: `options MAC_SEEOTHERUIDS`

Boot option: `mac_seeotheruids_load="YES"`

The mac_seeotheruids(4) module mimics and extends the `security.bsd.see_other_uids` and `security.bsd.see_other_gids` `sysctl` tunables. This option does not require any labels to be set before configuration and can operate transparently with the other modules.

After loading the module, the following `sysctl` tunables may be used to control the features:

- `security.mac.seeotheruids.enabled` will enable the module's features and use the default settings. These default settings will deny users the ability to view processes and sockets owned by other users.
- `security.mac.seeotheruids.specificgid_enabled` will allow a certain group to be exempt from this policy. To exempt specific groups from this policy, use the `security.mac.seeotheruids.specificgid=XXX` `sysctl` tunable. In the above example, the *XXX* should be replaced with the numeric group ID to be exempted.
- `security.mac.seeotheruids.primarygroup_enabled` is used to exempt specific primary groups from this policy. When using this tunable, the `security.mac.seeotheruids.specificgid_enabled` may not be set.

37.7. The MAC bsdextended Module

Module name: mac_bsdextended.ko

Kernel configuration line: `options MAC_BSDEXTENDED`

Boot option: `mac_bsdextended_load="YES"`

The mac_bsdextended(4) module enforces the file system firewall. This module's policy provides an extension to the standard file system permissions model, permitting an administrator to create a firewall-like ruleset to protect files, utilities, and directories in the file system hierarchy. When access to a file system object is attempted, the list of rules is iterated until either a matching rule is located or the end is reached. This behavior may be changed by the use of a sysctl(8) parameter, security.mac.bsdextended.firstmatch_enabled. Similar to other firewall modules in FreeBSD, a file containing access control rules can be created and read by the system at boot time using an rc.conf(5) variable.

The rule list may be entered using a utility, ugidfw(8), that has a syntax similar to that of ipfw(8). More tools can be written by using the functions in the libugidfw(3) library.

Extreme caution should be taken when working with this module; incorrect use could block access to certain parts of the file system.

37.7.1. Examples

After the mac_bsdextended(4) module has been loaded, the following command may be used to list the current rule configuration:

```
# ugidfw list
0 slots, 0 rules
```

As expected, there are no rules defined. This means that everything is still completely accessible. To create a rule which will block all access by users but leave `root` unaffected, simply run the following command:

```
# ugidfw add subject not uid root new object not uid root mode n
```

In releases prior to FreeBSD 5.3, the add parameter did not exist. In those cases the set should be used instead. See below for a command example.

This is a very bad idea as it will block all users from issuing even the most simple commands, such as `ls`. A more patriotic list of rules might be:

```
# ugidfw set 2 subject uid user1 object uid user2 mode n
# ugidfw set 3 subject uid user1 object gid user2 mode n
```

This will block any and all access, including directory listings, to `user2`'s home directory from the username `user1`.

In place of `user1`, the `not uid user2` could be passed. This will enforce the same access restrictions above for all users in place of just one user.

The `root` user will be unaffected by these changes.

This should provide a general idea of how the mac_bsdextended(4) module may be used to help fortify a file system. For more information, see the mac_bsdextended(4) and the ugidfw(8) manual pages.

37.8. The MAC ifoff Module

Module name: mac_ifoff.ko

Kernel configuration line: `options MAC_IFOFF`

Boot option: `mac_ifoff_load="YES"`

The mac_ifoff(4) module exists solely to disable network interfaces on the fly and keep network interfaces from being brought up during the initial system boot. It does not require any labels to be set up on the system, nor does it have a dependency on other MAC modules.

Most of the control is done through the `sysctl` tunables listed below.

- `security.mac.ifoff.lo_enabled` will enable/disable all traffic on the loopback (lo(4)) interface.
- `security.mac.ifoff.bpfrecv_enabled` will enable/disable all traffic on the Berkeley Packet Filter interface (bpf(4))
- `security.mac.ifoff.other_enabled` will enable/disable traffic on all other interfaces.

One of the most common uses of mac_ifoff(4) is network monitoring in an environment where network traffic should not be permitted during the boot sequence. Another suggested use would be to write a script which uses security/aide to automatically block network traffic if it finds new or altered files in protected directories.

37.9. The MAC portacl Module

Module name: mac_portacl.ko

Kernel configuration line: `MAC_PORTACL`

Boot option: `mac_portacl_load="YES"`

The mac_portacl(4) module is used to limit binding to local TCP and UDP ports using a variety of `sysctl` variables. In essence mac_portacl(4) makes it possible to allow non-`root` users to bind to specified privileged ports, i.e. ports fewer than 1024.

Once loaded, this module will enable the MAC policy on all sockets. The following tunables are available:

- `security.mac.portacl.enabled` will enable/disable the policy completely.
- `security.mac.portacl.port_high` will set the highest port number that mac_portacl(4) will enable protection for.
- `security.mac.portacl.suser_exempt` will, when set to a non-zero value, exempt the `root` user from this policy.
- `security.mac.portacl.rules` will specify the actual mac_portacl policy; see below.

The actual `mac_portacl` policy, as specified in the `security.mac.portacl.rules` sysctl, is a text string of the form: `rule[,rule,…]` with as many rules as needed. Each rule is of the form: `idtype:id:protocol:port`. The idtype parameter can be `uid` or `gid` and used to interpret the id parameter as either a user id or group id, respectively. The protocol parameter is used to determine if the rule should apply to TCP or UDP by setting the parameter to `tcp` or `udp`. The final port parameter is the port number to allow the specified user or group to bind to.

Since the ruleset is interpreted directly by the kernel only numeric values can be used for the user ID, group ID, and port parameters. I.e. user, group, and port service names cannot be used.

By default, on UNIX®-like systems, ports fewer than 1024 can only be used by/bound to privileged processes, i.e. those run as `root`. For mac_portacl(4) to allow non-privileged processes to bind to ports below 1024 this standard UNIX® restriction has to be disabled. This can be accomplished by setting the sysctl(8) variables `net.inet.ip.portrange.reservedlow` and `net.inet.ip.portrange.reservedhigh` to zero.

See the examples below or review the mac_portacl(4) manual page for further information.

37.9.1. Examples

The following examples should illuminate the above discussion a little better:

```
# sysctl security.mac.portacl.port_high=1023
# sysctl net.inet.ip.portrange.reservedlow=0 net.inet.ip.portrange.reservedhigh=0
```

First we set mac_portacl(4) to cover the standard privileged ports and disable the normal UNIX® bind restrictions.

```
# sysctl security.mac.portacl.suser_exempt=1
```

The `root` user should not be crippled by this policy, thus set the `security.mac.portacl.suser_exempt` to a non-zero value. The mac_portacl(4) module has now been set up to behave the same way UNIX®-like systems behave by default.

```
# sysctl security.mac.portacl.rules=uid:80:tcp:80
```

Allow the user with UID 80 (normally the `www` user) to bind to port 80. This can be used to allow the `www` user to run a web server without ever having `root` privilege.

```
# sysctl security.mac.portacl.rules=uid:1001:tcp:110,uid:1001:tcp:995
```

Permit the user with the UID of 1001 to bind to the TCP ports 110 ("pop3") and 995 ("pop3s"). This will permit this user to start a server that accepts connections on ports 110 and 995.

37.10. The MAC partition Module

Module name: mac_partition.ko

Kernel configuration line: `options MAC_PARTITION`

Boot option: `mac_partition_load="YES"`

The mac_partition(4) policy will drop processes into specific "partitions" based on their MAC label. Think of it as a special type of jail(8), though that is hardly a worthy comparison.

This is one module that should be added to the loader.conf(5) file so that it loads and enables the policy during the boot process.

Most configuration for this policy is done using the setpmac(8) utility which will be explained below. The following `sysctl` tunable is available for this policy:

- `security.mac.partition.enabled` will enable the enforcement of MAC process partitions.

When this policy is enabled, users will only be permitted to see their processes, and any others

within their partition, but will not be permitted to work with utilities outside the scope of this partition. For instance, a user in the `insecure` class above will not be permitted to access the `top` command as well as many other commands that must spawn a process.

To set or drop utilities into a partition label, use the `setpmac` utility:

```
# setpmac partition/13 top
```

This will add the `top` command to the label set on users in the `insecure` class. Note that all processes spawned by users in the `insecure` class will stay in the `partition/13` label.

37.10.1. Examples

The following command will show you the partition label and the process list:

```
# ps Zax
```

This next command will allow the viewing of another user's process partition label and that user's currently running processes:

```
# ps -ZU trhodes
```

Users can see processes in `root`'s label unless the mac_seeotheruids(4) policy is loaded.

A really crafty implementation could have all of the services disabled in /etc/rc.conf and started by a script that starts them with the proper labeling set.

The following policies support integer settings in place of the three default labels offered. These options, including their limitations, are further explained in the module manual pages.

37.11. The MAC Multi-Level Security Module

Module name: mac_mls.ko

Kernel configuration line: `options MAC_MLS`

Boot option: `mac_mls_load="YES"`

The mac_mls(4) policy controls access between subjects and objects in the system by enforcing a strict information flow policy.

In MLS environments, a "clearance" level is set in each subject or objects label, along with compartments. Since these clearance or sensibility levels can reach numbers greater than six thousand; it would be a daunting task for any system administrator to thoroughly configure each

subject or object. Thankfully, three "instant" labels are already included in this policy.

These labels are `mls/low`, `mls/equal` and `mls/high`. Since these labels are described in depth in the manual page, they will only get a brief description here:

- The `mls/low` label contains a low configuration which permits it to be dominated by all other objects. Anything labeled with `mls/low` will have a low clearance level and not be permitted to access information of a higher level. In addition, this label will prevent objects of a higher clearance level from writing or passing information on to them.
- The `mls/equal` label should be placed on objects considered to be exempt from the policy.
- The `mls/high` label is the highest level of clearance possible. Objects assigned this label will hold dominance over all other objects in the system; however, they will not permit the leaking of information to objects of a lower class.

MLS provides for:

- A hierarchical security level with a set of non hierarchical categories;
- Fixed rules: no read up, no write down (a subject can have read access to objects on its own level or below, but not above. Similarly, a subject can have write access to objects on its own level or above but not beneath.);
- Secrecy (preventing inappropriate disclosure of data);
- Basis for the design of systems that concurrently handle data at multiple sensitivity levels (without leaking information between secret and confidential).

The following `sysctl` tunables are available for the configuration of special services and interfaces:

- `security.mac.mls.enabled` is used to enable/disable the MLS policy.
- `security.mac.mls.ptys_equal` will label all pty(4) devices as `mls/equal` during creation.
- `security.mac.mls.revocation_enabled` is used to revoke access to objects after their label changes to a label of a lower grade.
- `security.mac.mls.max_compartments` is used to set the maximum number of compartment levels with objects; basically the maximum compartment number allowed on a system.

To manipulate the MLS labels, the setfmac(8) command has been provided. To assign a label to an object, issue the following command:

```
# setfmac mls/5 test
```

To get the MLS label for the file test issue the following command:

```
# getfmac test
```

This is a summary of the MLS policy's features. Another approach is to create a master policy file in /etc which specifies the MLS policy information and to feed that file into the `setfmac` command. This

method will be explained after all policies are covered.

37.11.1. Planning Mandatory Sensitivity

With the Multi-Level Security Policy Module, an administrator plans for controlling the flow of sensitive information. By default, with its block read up block write down nature, the system defaults everything to a low state. Everything is accessible and an administrator slowly changes this during the configuration stage; augmenting the confidentiality of the information.

Beyond the three basic label options above, an administrator may group users and groups as required to block the information flow between them. It might be easier to look at the information in clearance levels familiarized with words, for instance classifications such as `Confidential`, `Secret`, and `Top Secret`. Some administrators might just create different groups based on project levels. Regardless of classification method, a well thought out plan must exist before implementing such a restrictive policy.

Some example situations for this security policy module could be an e-commerce web server, a file server holding critical company information, and financial institution environments. The most unlikely place would be a personal workstation with only two or three users.

37.12. The MAC Biba Module

Module name: mac_biba.ko

Kernel configuration line: `options MAC_BIBA`

Boot option: `mac_biba_load="YES"`

The mac_biba(4) module loads the MAC Biba policy. This policy works much like that of the MLS policy with the exception that the rules for information flow are slightly reversed. This is said to prevent the downward flow of sensitive information whereas the MLS policy prevents the upward flow of sensitive information; thus, much of this section can apply to both policies.

In Biba environments, an "integrity" label is set on each subject or object. These labels are made up of hierarchal grades, and non-hierarchal components. As an object's or subject's grade ascends, so does its integrity.

Supported labels are `biba/low`, `biba/equal`, and `biba/high`; as explained below:

- The `biba/low` label is considered the lowest integrity an object or subject may have. Setting this on objects or subjects will block their write access to objects or subjects marked high. They still have read access though.
- The `biba/equal` label should only be placed on objects considered to be exempt from the policy.
- The `biba/high` label will permit writing to objects set at a lower label, but not permit reading that object. It is recommended that this label be placed on objects that affect the integrity of the entire system.

Biba provides for:

- Hierarchical integrity level with a set of non hierarchical integrity categories;
- Fixed rules: no write up, no read down (opposite of MLS). A subject can have write access to objects on its own level or below, but not above. Similarly, a subject can have read access to objects on its own level or above, but not below;
- Integrity (preventing inappropriate modification of data);
- Integrity levels (instead of MLS sensitivity levels).

The following `sysctl` tunables can be used to manipulate the Biba policy.

- `security.mac.biba.enabled` may be used to enable/disable enforcement of the Biba policy on the target machine.
- `security.mac.biba.ptys_equal` may be used to disable the Biba policy on pty(4) devices.
- `security.mac.biba.revocation_enabled` will force the revocation of access to objects if the label is changed to dominate the subject.

To access the Biba policy setting on system objects, use the `setfmac` and `getfmac` commands:

```
# setfmac biba/low test
# getfmac test
test: biba/low
```

37.12.1. Planning Mandatory Integrity

Integrity, different from sensitivity, guarantees that the information will never be manipulated by untrusted parties. This includes information passed between subjects, objects, and both. It ensures that users will only be able to modify and in some cases even access information they explicitly need to.

The mac_biba(4) security policy module permits an administrator to address which files and programs a user or users may see and invoke while assuring that the programs and files are free from threats and trusted by the system for that user, or group of users.

During the initial planning phase, an administrator must be prepared to partition users into grades, levels, and areas. Users will be blocked access not only to data but programs and utilities both before and after they start. The system will default to a high label once this policy module is enabled, and it is up to the administrator to configure the different grades and levels for users. Instead of using clearance levels as described above, a good planning method could include topics. For instance, only allow developers modification access to the source code repository, source code compiler, and other development utilities. While other users would be grouped into other categories such as testers, designers, or just ordinary users and would only be permitted read access.

With its natural security control, a lower integrity subject is unable to write to a higher integrity subject; a higher integrity subject cannot observe or read a lower integrity object. Setting a label at the lowest possible grade could make it inaccessible to subjects. Some prospective environments for this security policy module would include a constrained web server, development and test

machine, and source code repository. A less useful implementation would be a personal workstation, a machine used as a router, or a network firewall.

37.13. The MAC LOMAC Module

Module name: mac_lomac.ko

Kernel configuration line: `options MAC_LOMAC`

Boot option: `mac_lomac_load="YES"`

Unlike the MAC Biba policy, the mac_lomac(4) policy permits access to lower integrity objects only after decreasing the integrity level to not disrupt any integrity rules.

The MAC version of the Low-watermark integrity policy, not to be confused with the older lomac(4) implementation, works almost identically to Biba, but with the exception of using floating labels to support subject demotion via an auxiliary grade compartment. This secondary compartment takes the form of `[auxgrade]`. When assigning a lomac policy with an auxiliary grade, it should look a little bit like: `lomac/10[2]` where the number two (2) is the auxiliary grade.

The MAC LOMAC policy relies on the ubiquitous labeling of all system objects with integrity labels, permitting subjects to read from low integrity objects and then downgrading the label on the subject to prevent future writes to high integrity objects. This is the `[auxgrade]` option discussed above, thus the policy may provide for greater compatibility and require less initial configuration than Biba.

37.13.1. Examples

Like the Biba and MLS policies; the `setfmac` and `setpmac` utilities may be used to place labels on system objects:

```
# setfmac /usr/home/trhodes lomac/high[low]
# getfmac /usr/home/trhodes
lomac/high[low]
```

Notice the auxiliary grade here is `low`, this is a feature provided only by the MAC LOMAC policy.

37.14. Nagios in a MAC Jail

The following demonstration will implement a secure environment using various MAC modules with properly configured policies. This is only a test and should not be considered the complete answer to everyone's security woes. Just implementing a policy and ignoring it never works and could be disastrous in a production environment.

Before beginning this process, the `multilabel` option must be set on each file system as stated at the beginning of this chapter. Not doing so will result in errors. While at it, ensure that the net-mngt/nagios-plugins, net-mngt/nagios, and www/apache13 ports are all installed, configured, and working correctly.

37.14.1. Create an insecure User Class

Begin the procedure by adding the following user class to the /etc/login.conf file:

```
insecure:\
:welcome=/etc/motd:\
:setenv=MAIL=/var/mail/$,BLOCKSIZE=K:\
:path=~/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/sbin:/usr/local/bin
:manpath=/usr/shared/man /usr/local/man:\
:nologin=/usr/sbin/nologin:\
:cputime=1h30m:\
:datasize=8M:\
:vmemoryuse=100M:\
:stacksize=2M:\
:memorylocked=4M:\
:memoryuse=8M:\
:filesize=8M:\
:coredumpsize=8M:\
:openfiles=24:\
:maxproc=32:\
:priority=0:\
:requirehome:\
:passwordtime=91d:\
:umask=022:\
:ignoretime@:\
:label=biba/10(10-10):
```

And adding the following line to the default user class:

```
:label=biba/high:
```

Once this is completed, the following command must be issued to rebuild the database:

```
# cap_mkdb /etc/login.conf
```

37.14.2. Boot Configuration

Do not reboot yet, just add the following lines to /boot/loader.conf so the required modules will load during system initialization:

```
mac_biba_load="YES"
mac_seeotheruids_load="YES"
```

37.14.3. Configure Users

Set the `root` user to the default class using:

```
# pw usermod root -L default
```

All user accounts that are not `root` or system users will now require a login class. The login class is required otherwise users will be refused access to common commands such as vi(1). The following `sh` script should do the trick:

```
# for x in `awk -F: '($3 >= 1001) && ($3 != 65534) { print $1 }' \

# /etc/passwd`; do pw usermod $x -L default; done;
```

Drop the `nagios` and `www` users into the insecure class:

```
# pw usermod nagios -L insecure
```

```
# pw usermod www -L insecure
```

37.14.4. Create the Contexts File

A contexts file should now be created; the following example file should be placed in /etc/policy.contexts.

```
# This is the default BIBA policy for this system.

# System:
/var/run                        biba/equal
/var/run/*                      biba/equal

/dev                            biba/equal
/dev/*                          biba/equal

/var                biba/equal
/var/spool                      biba/equal
/var/spool/*                    biba/equal

/var/log                        biba/equal
/var/log/*                      biba/equal

/tmp                biba/equal
/tmp/*              biba/equal
/var/tmp            biba/equal
/var/tmp/*          biba/equal
```

```
/var/spool/mqueue       biba/equal
/var/spool/clientmqueue     biba/equal

# For Nagios:
/usr/local/etc/nagios
/usr/local/etc/nagios/*         biba/10

/var/spool/nagios               biba/10
/var/spool/nagios/*             biba/10

# For apache
/usr/local/etc/apache           biba/10
/usr/local/etc/apache/*         biba/10
```

This policy will enforce security by setting restrictions on the flow of information. In this specific configuration, users, `root` and others, should never be allowed to access Nagios. Configuration files and processes that are a part of Nagios will be completely self contained or jailed.

This file may now be read into our system by issuing the following command:

```
# setfsmac -ef /etc/policy.contexts /
# setfsmac -ef /etc/policy.contexts /
```

The above file system layout may be different depending on environment; however, it must be run on every single file system.

The /etc/mac.conf file requires the following modifications in the main section:

```
default_labels file ?biba
default_labels ifnet ?biba
default_labels process ?biba
default_labels socket ?biba
```

37.14.5. Enable Networking

Add the following line to /boot/loader.conf:

```
security.mac.biba.trust_all_interfaces=1
```

And the following to the network card configuration stored in rc.conf. If the primary Internet configuration is done via DHCP, this may need to be configured manually after every system boot:

```
maclabel biba/equal
```

37.14.6. Testing the Configuration

Ensure that the web server and Nagios will not be started on system initialization, and reboot. Ensure the `root` user cannot access any of the files in the Nagios configuration directory. If `root` can issue an ls(1) command on /var/spool/nagios, then something is wrong. Otherwise a "permission denied" error should be returned.

If all seems well, Nagios, Apache, and Sendmail can now be started in a way fitting of the security policy. The following commands will make this happen:

```
# cd /etc/mail && make stop && \
setpmac biba/equal make start && setpmac biba/10\(10-10\) apachectl start && \
setpmac biba/10\(10-10\) /usr/local/etc/rc.d/nagios.sh forcestart
```

Double check to ensure that everything is working properly. If not, check the log files or error messages. Use the sysctl(8) utility to disable the mac_biba(4) security policy module enforcement and try starting everything again, like normal.

The `root` user can change the security enforcement and edit the configuration files without fear. The following command will permit the degradation of the security policy to a lower grade for a newly spawned shell:

```
# setpmac biba/10 csh
```

To block this from happening, force the user into a range via login.conf(5). If setpmac(8) attempts to run a command outside of the compartment's range, an error will be returned and the command will not be executed. In this case, setting root to `biba/high(high-high)`.

37.15. User Lock Down

This example considers a relatively small, fewer than fifty users, storage system. Users would have login capabilities, and be permitted to not only store data but access resources as well.

For this scenario, the mac_bsdextended(4) mixed with mac_seeotheruids(4) could co-exist and block access not only to system objects but to hide user processes as well.

Begin by adding the following lines to /boot/loader.conf:

```
mac_seeotheruids_enabled="YES"
```

The mac_bsdextended(4) security policy module may be activated through the use of the following rc.conf variable:

```
ugidfw_enable="YES"
```

Default rules stored in /etc/rc.bsdextended will be loaded at system initialization; however, the default entries may need modification. Since this machine is expected only to service users, everything may be left commented out except the last two. These will force the loading of user owned system objects by default.

Add the required users to this machine and reboot. For testing purposes, try logging in as a different user across two consoles. Run the `ps aux` command to see if processes of other users are visible. Try to run ls(1) on another users home directory, it should fail.

Do not try to test with the `root` user unless the specific `sysctl`s have been modified to block super user access.

When a new user is added, their mac_bsdextended(4) rule will not be in the ruleset list. To update the ruleset quickly, simply unload the security policy module and reload it again using the kldunload(8) and kldload(8) utilities.

37.16. Troubleshooting the MAC Framework

During the development stage, a few users reported problems with normal configuration. Some of these problems are listed below:

37.16.1. The `multilabel` option cannot be enabled on /

The `multilabel` flag does not stay enabled on my root (/) partition!

It seems that one out of every fifty users has this problem, indeed, we had this problem during our initial configuration. Further observation of this so called "bug" has lead me to believe that it is a result of either incorrect documentation or misinterpretation of the documentation. Regardless of why it happened, the following steps may be taken to resolve it:

1. Edit /etc/fstab and set the root partition at `ro` for read-only.
2. Reboot into single user mode.
3. Run `tunefs -l enable` on /.
4. Reboot the system into normal mode.
5. Run `mount -urw` / and change the `ro` back to `rw` in /etc/fstab and reboot the system again.
6. Double-check the output from the `mount` to ensure that `multilabel` has been properly set on the root file system.

37.16.2. Cannot start a X11 server after MAC

After establishing a secure environment with MAC, I am no longer able to start X!

This could be caused by the MAC `partition` policy or by a mislabeling in one of the MAC labeling

policies. To debug, try the following:

1. Check the error message; if the user is in the `insecure` class, the `partition` policy may be the culprit. Try setting the user's class back to the `default` class and rebuild the database with the `cap_mkdb` command. If this does not alleviate the problem, go to step two.
2. Double-check the label policies. Ensure that the policies are set correctly for the user in question, the X11 application, and the /dev entries.
3. If neither of these resolve the problem, send the error message and a description of your environment to the TrustedBSD discussion lists located at the TrustedBSD website or to the ηλεκτρονική λίστα γενικών ερωτήσεων του FreeBSD mailing list.

37.16.3. Error: _secure_path(3) cannot stat .login_conf

When I attempt to switch from the `root` to another user in the system, the error message `_secure_path: unable to state .login_conf`.

This message is usually shown when the user has a higher label setting then that of the user whom they are attempting to become. For instance a user on the system, `joe`, has a default label of `biba/low`. The `root` user, who has a label of `biba/high`, cannot view `joe`'s home directory. This will happen regardless if `root` has used the `su` command to become `joe`, or not. In this scenario, the Biba integrity model will not permit `root` to view objects set at a lower integrity level.

37.16.4. The `root` username is broken!

In normal or even single user mode, the `root` is not recognized. The `whoami` command returns 0 (zero) and `su` returns `who are you?`. What could be going on?

This can happen if a labeling policy has been disabled, either by a sysctl(8) or the policy module was unloaded. If the policy is being disabled or has been temporarily disabled, then the login capabilities database needs to be reconfigured with the `label` option being removed. Double check the login.conf file to ensure that all `label` options have been removed and rebuild the database with the `cap_mkdb` command.

This may also happen if a policy restricts access to the master.passwd file or database. Usually caused by an administrator altering the file under a label which conflicts with the general policy being used by the system. In these cases, the user information would be read by the system and access would be blocked as the file has inherited the new label. Disable the policy via a sysctl(8) and everything should return to normal.

Chapter 38. Έλεγχος Συμβάντων Ασφαλείας

38.1. Σύνοψη

Οι εκδόσεις του FreeBSD από την 6.2-RELEASE και μετά περιλαμβάνουν υποστήριξη για λεπτομερή έλεγχο συμβάντων ασφαλείας. Ο έλεγχος συμβάντων επιτρέπει αξιόπιστη, λεπτομερή και παραμετροποιήσιμη καταγραφή πλήθους συμβάντων σχετικών με την ασφάλεια, συμπεριλαμβανομένων των logins, των αλλαγών ρυθμίσεων, καθώς και της πρόσβασης σε αρχεία και στο δίκτυο. Οι καταγραφές αυτές είναι πολύτιμες για απευθείας παρακολούθηση του συστήματος, ανίχνευση εισβολέων, καθώς και για ανάλυση μετά από κάποια επίθεση. Το FreeBSD υλοποιεί τη μορφή αρχείων και το BSM API όπως έχουν δημοσιευτεί από την Sun™, και επιτρέπει διαλειτουργικότητα με τις υλοποιήσεις ελέγχου τόσο του Solaris™ της Sun™ όσο του Mac OS® της Apple®.

Το κεφάλαιο αυτό εστιάζει στην εγκατάσταση και ρύθμιση του Ελέγχου Συμβάντων. Εξηγεί τις πολιτικές ελέγχου, και παρέχει ένα παράδειγμα ρυθμίσεων ελέγχου.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τι είναι ο έλεγχος συμβάντων και πως λειτουργεί.
- Πως να ρυθμίσετε τον έλεγχο συμβάντων στο FreeBSD για χρήστες και προγράμματα (processes).
- Πως να αναλύσετε τα ίχνη του ελέγχου χρησιμοποιώντας τα εργαλεία μείωσης όγκου δεδομένων και ανάλυσης.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε τις βασικές έννοιες του UNIX® και του FreeBSD (Βασικές Έννοιες στο UNIX®).
- Να είστε εξοικειωμένος με τις βασικές έννοιες της ρύθμισης και μεταγλώττισης του πυρήνα. (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να έχετε κάποια εξοικείωση με την ασφάλεια και πως αυτή σχετίζεται με το FreeBSD (Ασφάλεια).

Οι λειτουργίες ελέγχου στο FreeBSD 6.2 είναι σε πειραματικό στάδιο και η εγκατάσταση τους σε μηχανήματα παραγωγής θα πρέπει να γίνεται μόνο αφού ληφθούν σοβαρά υπόψιν οι κίνδυνοι από την εγκατάσταση πειραματικού λογισμικού. Οι γνωστοί αυτή τη στιγμή τρέχοντες περιορισμοί περιλαμβάνουν την αδυναμία ελέγχου όλων των συμβάντων που σχετίζονται με την ασφάλεια. Επίσης κάποιοι μηχανισμοί εισόδου (logins), όπως οι γραφικοί (X11-βασισμένοι) display managers, καθώς και ορισμένες υπηρεσίες τρίτων κατασκευαστών δεν είναι σωστά ρυθμισμένες για τον έλεγχο εισόδου χρηστών.

Ο έλεγχος συμβάντων ασφαλείας μπορεί να δημιουργήσει πολύ λεπτομερείς καταγραφές της δραστηριότητας του συστήματος: σε ένα σύστημα με υψηλό φόρτο, τα αρχεία καταγραφής μπορεί να γίνουν πολύ μεγάλα, αν έχουν ρυθμιστεί για λεπτομερή καταγραφή, και να ξεπεράσουν τα αρκετά gigabytes την εβδομάδα σε κάποιες περιπτώσεις. Οι διαχειριστές θα πρέπει να λαμβάνουν υπόψιν τους τις

πιθανές απαιτήσεις σε χώρο δίσκου σε περίπτωση ρυθμίσεων λεπτομερούς καταγραφής. Για παράδειγμα, ίσως είναι θεμιτό να αφιερωθεί ένα σύστημα αρχείων στο /var/audit ώστε τα υπόλοιπα συστήματα αρχείων να μην επηρεαστούν αν ο χώρος αυτός εξαντληθεί.

38.2. Key Terms in this Chapter

Before reading this chapter, a few key audit-related terms must be explained:

- *event*: An auditable event is any event that can be logged using the audit subsystem. Examples of security-relevant events include the creation of a file, the building of a network connection, or a user logging in. Events are either "attributable", meaning that they can be traced to an authenticated user, or "non-attributable" if they cannot be. Examples of non-attributable events are any events that occur before authentication in the login process, such as bad password attempts.
- *class*: Event classes are named sets of related events, and are used in selection expressions. Commonly used classes of events include "file creation" (fc), "exec" (ex) and "login_logout" (lo).
- *record*: A record is an audit log entry describing a security event. Records contain a record event type, information on the subject (user) performing the action, date and time information, information on any objects or arguments, and a success or failure condition.
- *trail*: An audit trail, or log file, consists of a series of audit records describing security events. Typically, trails are in roughly chronological order with respect to the time events completed. Only authorized processes are allowed to commit records to the audit trail.
- *selection expression*: A selection expression is a string containing a list of prefixes and audit event class names used to match events.
- *preselection*: The process by which the system identifies which events are of interest to the administrator in order to avoid generating audit records describing events that are not of interest. The preselection configuration uses a series of selection expressions to identify which classes of events to audit for which users, as well as global settings that apply to both authenticated and unauthenticated processes.
- *reduction*: The process by which records from existing audit trails are selected for preservation, printing, or analysis. Likewise, the process by which undesired audit records are removed from the audit trail. Using reduction, administrators can implement policies for the preservation of audit data. For example, detailed audit trails might be kept for one month, but after that, trails might be reduced in order to preserve only login information for archival purposes.

38.3. Installing Audit Support

User space support for Event Auditing is installed as part of the base FreeBSD operating system as of 6.2-RELEASE. However, Event Auditing support must be explicitly compiled into the kernel by adding the following lines to the kernel configuration file:

```
options AUDIT
```

Rebuild and reinstall the kernel via the normal process explained in Ρυθμίζοντας τον Πυρήνα του FreeBSD.

Once the kernel is built, installed, and the system has been rebooted, enable the audit daemon by adding the following line to rc.conf(5):

```
auditd_enable="YES"
```

Audit support must then be started by a reboot, or by manually starting the audit daemon:

```
/etc/rc.d/auditd start
```

38.4. Audit Configuration

All configuration files for security audit are found in /etc/security. The following files must be present before the audit daemon is started:

- audit_class - Contains the definitions of the audit classes.
- audit_control - Controls aspects of the audit subsystem, such as default audit classes, minimum disk space to leave on the audit log volume, maximum audit trail size, etc.
- audit_event - Textual names and descriptions of system audit events, as well as a list of which classes each event in in.
- audit_user - User-specific audit requirements, which are combined with the global defaults at login.
- audit_warn - A customizable shell script used by auditd to generate warning messages in exceptional situations, such as when space for audit records is running low or when the audit trail file has been rotated.

Audit configuration files should be edited and maintained carefully, as errors in configuration may result in improper logging of events.

38.4.1. Event Selection Expressions

Selection expressions are used in a number of places in the audit configuration to determine which events should be audited. Expressions contain a list of event classes to match, each with a prefix indicating whether matching records should be accepted or ignored, and optionally to indicate if the entry is intended to match successful or failed operations. Selection expressions are evaluated from left to right, and two expressions are combined by appending one onto the other.

The following list contains the default audit event classes present in audit_class:

- `all` - `all` - Match all event classes.
- `ad` - `administrative` - Administrative actions performed on the system as a whole.
- `ap` - `application` - Application defined action.

- `cl` - `file_close` - Audit calls to the `close` system call.
- `ex` - `exec` - Audit program execution. Auditing of command line arguments and environmental variables is controlled via audit_control(5) using the `argv` and `envv` parameters to the `policy` setting.
- `fa` - `file_attr_acc` - Audit the access of object attributes such as stat(1), pathconf(2) and similar events.
- `fc` - `file_creation` - Audit events where a file is created as a result.
- `fd` - `file_deletion` - Audit events where file deletion occurs.
- `fm` - `file_attr_mod` - Audit events where file attribute modification occurs, such as chown(8), chflags(1), flock(2), etc.
- `fr` - `file_read` - Audit events in which data is read, files are opened for reading, etc.
- `fw` - `file_write` - Audit events in which data is written, files are written or modified, etc.
- `io` - `ioctl` - Audit use of the ioctl(2) system call.
- `ip` - `ipc` - Audit various forms of Inter-Process Communication, including POSIX pipes and System V IPC operations.
- `lo` - `login_logout` - Audit login(1) and logout(1) events occurring on the system.
- `na` - `non_attrib` - Audit non-attributable events.
- `no` - `no_class` - Match no audit events.
- `nt` - `network` - Audit events related to network actions, such as connect(2) and accept(2).
- `ot` - `other` - Audit miscellaneous events.
- `pc` - `process` - Audit process operations, such as exec(3) and exit(3).

These audit event classes may be customized by modifying the audit_class and audit_event configuration files.

Each audit class in the list is combined with a prefix indicating whether successful/failed operations are matched, and whether the entry is adding or removing matching for the class and type.

- (none) Audit both successful and failed instances of the event.
- `+` Audit successful events in this class.
- `-` Audit failed events in this class.
- `^` Audit neither successful nor failed events in this class.
- `^+` Don't audit successful events in this class.
- `^-` Don't audit failed events in this class.

The following example selection string selects both successful and failed login/logout events, but only successful execution events:

```
lo,+ex
```

38.4.2. Configuration Files

In most cases, administrators will need to modify only two files when configuring the audit system: audit_control and audit_user. The first controls system-wide audit properties and policies; the second may be used to fine-tune auditing by user.

38.4.2.1. The audit_control File

The audit_control file specifies a number of defaults for the audit subsystem. Viewing the contents of this file, we see the following:

```
dir:/var/audit
flags:lo
minfree:20
naflags:lo
policy:cnt
filesz:0
```

The `dir` option is used to set one or more directories where audit logs will be stored. If more than one directory entry appears, they will be used in order as they fill. It is common to configure audit so that audit logs are stored on a dedicated file system, in order to prevent interference between the audit subsystem and other subsystems if the file system fills.

The `flags` field sets the system-wide default preselection mask for attributable events. In the example above, successful and failed login and logout events are audited for all users.

The `minfree` option defines the minimum percentage of free space for the file system where the audit trail is stored. When this threshold is exceeded, a warning will be generated. The above example sets the minimum free space to twenty percent.

The `naflags` option specifies audit classes to be audited for non-attributed events, such as the login process and system daemons.

The `policy` option specifies a comma-separated list of policy flags controlling various aspects of audit behavior. The default `cnt` flag indicates that the system should continue running despite an auditing failure (this flag is highly recommended). Another commonly used flag is `argv`, which causes command line arguments to the execve(2) system call to audited as part of command execution.

The `filesz` option specifies the maximum size in bytes to allow an audit trail file to grow to before automatically terminating and rotating the trail file. The default, 0, disables automatic log rotation. If the requested file size is non-zero and below the minimum 512k, it will be ignored and a log message will be generated.

38.4.2.2. The audit_user File

The audit_user file permits the administrator to specify further audit requirements for specific users. Each line configures auditing for a user via two fields: the first is the `alwaysaudit` field, which specifies a set of events that should always be audited for the user, and the second is the `neveraudit`

field, which specifies a set of events that should never be audited for the user.

The following example audit_user file audits login/logout events and successful command execution for the root user, and audits file creation and successful command execution for the www user. If used with the example audit_control file above, the `lo` entry for `root` is redundant, and login/logout events will also be audited for the `www` user.

```
root:lo,+ex:no
www:fc,+ex:no
```

38.5. Administering the Audit Subsystem

38.5.1. Viewing Audit Trails

Audit trails are stored in the BSM binary format, so tools must be used to modify or convert to text. The `praudit` command convert trail files to a simple text format; the `auditreduce` command may be used to reduce the audit trail file for analysis, archiving, or printing purposes. `auditreduce` supports a variety of selection parameters, including event type, event class, user, date or time of the event, and the file path or object acted on.

For example, the `praudit` utility will dump the entire contents of a specified audit log in plain text:

```
# praudit /var/audit/AUDITFILE
```

Where *AUDITFILE* is the audit log to dump.

Audit trails consist of a series of audit records made up of tokens, which `praudit` prints sequentially one per line. Each token is of a specific type, such as `header` holding an audit record header, or `path` holding a file path from a name lookup. The following is an example of an `execve` event:

```
header,133,10,execve(2),0,Mon Sep 25 15:58:03 2006, + 384 msec
exec arg,finger,doug
path,/usr/bin/finger
attribute,555,root,wheel,90,24918,104944
subject,robert,root,wheel,root,wheel,38439,38032,42086,128.232.9.100
return,success,0
trailer,133
```

This audit represents a successful `execve` call, in which the command `finger doug` has been run. The arguments token contains both the processed command line presented by the shell to the kernel. The path token holds the path to the executable as looked up by the kernel. The attribute token describes the binary, and in particular, includes the file mode which can be used to determine if the application was setuid. The subject token describes the subject process, and stores in sequence the audit user ID, effective user ID and group ID, real user ID and group ID, process ID, session ID, port ID, and login address. Notice that the audit user ID and real user ID differ: the user `robert` has switched to the `root` account before running this command, but it is audited using the original

authenticated user. Finally, the return token indicates the successful execution, and the trailer concludes the record.

38.5.2. Reducing Audit Trails

Since audit logs may be very large, an administrator will likely want to select a subset of records for using, such as records associated with a specific user:

```
# auditreduce -u trhodes /var/audit/AUDITFILE | praudit
```

This will select all audit records produced for the user `trhodes` stored in the AUDITFILE file.

38.5.3. Delegating Audit Review Rights

Members of the `audit` group are given permission to read audit trails in /var/audit; by default, this group is empty, so only the `root` user may read audit trails. Users may be added to the `audit` group in order to delegate audit review rights to the user. As the ability to track audit log contents provides significant insight into the behavior of users and processes, it is recommended that the delegation of audit review rights be performed with caution.

38.5.4. Live Monitoring Using Audit Pipes

Audit pipes are cloning pseudo-devices in the device file system which allow applications to tap the live audit record stream. This is primarily of interest to authors of intrusion detection and system monitoring applications. However, for the administrator the audit pipe device is a convenient way to allow live monitoring without running into problems with audit trail file ownership or log rotation interrupting the event stream. To track the live audit event stream, use the following command line

```
# praudit /dev/auditpipe
```

By default, audit pipe device nodes are accessible only to the `root` user. To make them accessible to the members of the `audit` group, add a `devfs` rule to devfs.rules:

```
add path 'auditpipe*' mode 0440 group audit
```

See devfs.rules(5) for more information on configuring the devfs file system.

It is easy to produce audit event feedback cycles, in which the viewing of each audit event results in the generation of more audit events. For example, if all network I/O is audited, and praudit is run from an SSH session, then a continuous stream of audit events will be generated at a high rate, as each event being printed will generate another event. It is advisable to run praudit on an audit pipe device from sessions without fine-grained I/O auditing in order to avoid this happening.

38.5.5. Rotating Audit Trail Files

Audit trails are written to only by the kernel, and managed only by the audit daemon, auditd. Administrators should not attempt to use newsyslog.conf(5) or other tools to directly rotate audit logs. Instead, the `audit` management tool may be used to shut down auditing, reconfigure the audit system, and perform log rotation. The following command causes the audit daemon to create a new audit log and signal the kernel to switch to using the new log. The old log will be terminated and renamed, at which point it may then be manipulated by the administrator.

```
# audit -n
```

If the auditd daemon is not currently running, this command will fail and an error message will be produced.

Adding the following line to /etc/crontab will force the rotation every twelve hours from cron(8):

```
0     */12      *       *       *       root    /usr/sbin/audit -n
```

The change will take effect once you have saved the new /etc/crontab.

Automatic rotation of the audit trail file based on file size is possible via the `filesz` option in audit_control(5), and is described in the configuration files section of this chapter.

38.5.6. Compressing Audit Trails

As audit trail files can become very large, it is often desirable to compress or otherwise archive trails once they have been closed by the audit daemon. The audit_warn script can be used to perform customized operations for a variety of audit-related events, including the clean termination of audit trails when they are rotated. For example, the following may be added to the audit_warn script to compress audit trails on close:

```
#
# Compress audit trail files on close.
#
if [ "$1" = closefile ]; then
        gzip -9 $2
fi
```

Other archiving activities might include copying trail files to a centralized server, deleting old trail files, or reducing the audit trail to remove unneeded records. The script will be run only when audit trail files are cleanly terminated, so will not be run on trails left unterminated following an improper shutdown.

Chapter 39. Αποθηκευτικά Μέσα

39.1. Σύνοψη

Το κεφάλαιο αυτό καλύπτει την χρήση των δίσκων στο FreeBSD. Περιλαμβάνει δίσκους που υποστηρίζονται από μνήμη, δίσκους συνδεδεμένους απευθείας στο δίκτυο, τις τυπικές συσκευές αποθήκευσης SCSI/IDE, καθώς και συσκευές που χρησιμοποιούν διεπαφή USB.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Την ορολογία που χρησιμοποιεί το FreeBSD για να περιγράψει την οργάνωση των δεδομένων στο φυσικό μέσο του δίσκου (partitions - κατατμήσεις - και slices).
- Πως να προσθέσετε νέους σκληρούς δίσκους στο σύστημα σας.
- Πως να ρυθμίσετε το FreeBSD να χρησιμοποιεί συσκευές αποθήκευσης USB.
- Πως να ρυθμίσετε εικονικά συστήματα αρχείων, όπως δίσκους που αποθηκεύονται σε μνήμη RAM.
- Πως να χρησιμοποιήσετε quotas για να περιορίσετε τη χρήση χώρου στο δίσκο.
- Πως να κρυπτογραφήσετε δίσκους για να τους ασφαλίσετε από επιθέσεις.
- Πως να δημιουργήσετε και να γράψετε CD και DVD στο FreeBSD.
- Πως να χρησιμοποιήσετε προγράμματα λήψης αντιγράφων ασφαλείας στο FreeBSD.
- Τι είναι οι εικόνες (snapshots) σε ένα σύστημα αρχείων και πως να τις χρησιμοποιήσετε αποδοτικά.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ξέρετε πως να ρυθμίσετε και να εγκαταστήσετε ένα νέο πυρήνα του FreeBSD.

39.2. Device Names

The following is a list of physical storage devices supported in FreeBSD and their associated device names.

Πίνακας 3. Physical Disk Naming Conventions

Drive type	Drive device name
IDE hard drives	`ad` or `ada`
IDE CD-ROM drives	`acd` or `cd`
SATA hard drives	`ad` or `ada`
SATA CD-ROM drives	`acd` or `cd`
SCSI hard drives and USB Mass storage devices	`da`
SCSI CD-ROM drives	`cd`

Drive type	Drive device name
Assorted non-standard CD-ROM drives	`mcd` for Mitsumi CD-ROM and `scd` for Sony CD-ROM devices
Floppy drives	`fd`
SCSI tape drives	`sa`
IDE tape drives	`ast`
Flash drives	`fla` for DiskOnChip® Flash device
RAID drives	`aacd` for Adaptec® AdvancedRAID, `mlxd` and `mlyd` for Mylex®, `amrd` for AMI MegaRAID®, `idad` for Compaq Smart RAID, `twed` for 3ware® RAID.

39.3. Adding Disks

This section describes how to add a new SATA disk to a machine that currently only has a single drive. First, turn off the computer and install the drive in the computer following the instructions of the computer, controller, and drive manufacturers. Reboot the system and become `root`.

Inspect /var/run/dmesg.boot to ensure the new disk was found. In this example, the newly added SATA drive will appear as ada1.

For this example, a single large partition will be created on the new disk. The GPT partitioning scheme will be used in preference to the older and less versatile MBR scheme.

If the disk to be added is not blank, old partition information can be removed with `gpart delete`. See gpart(8) for details.

The partition scheme is created, and then a single partition is added:

```
# gpart create -s GPT ada1
# gpart add -t freebsd-ufs ada1
```

Depending on use, several smaller partitions may be desired. See gpart(8) for options to create partitions smaller than a whole disk.

A file system is created on the new blank disk:

```
# newfs -U /dev/ada1p1
```

An empty directory is created as a *mountpoint*, a location for mounting the new disk in the original disk's file system:

```
# mkdir /newdisk
```

Finally, an entry is added to /etc/fstab so the new disk will be mounted automatically at startup:

```
/dev/ada1p1 /newdisk    ufs rw  2   2
```

The new disk can be mounted manually, without restarting the system:

```
# mount /newdisk
```

39.4. USB Storage Devices

Many external storage solutions, such as hard drives, USB thumbdrives, and CD/DVD burners, use the Universal Serial Bus (USB). FreeBSD provides support for these devices.

39.4.1. Configuration

The USB mass storage devices driver, umass(4), is built into the GENERIC kernel and provides support for USB storage devices. For a custom kernel, be sure that the following lines are present in the kernel configuration file:

```
device scbus
device da
device pass
device uhci
device ohci
device ehci
device usb
device umass
```

Since the umass(4) driver uses the SCSI subsystem to access the USB storage devices, any USB device will be seen as a SCSI device by the system. Depending on the USB chipset on the motherboard, `device uhci` or `device ohci` is used to provide USB 1.X support. Support for USB 2.0 controllers is provided by `device ehci`.

If the USB device is a CD or DVD burner, cd(4), must be added to the kernel via the line:

```
device cd
```

Since the burner is seen as a SCSI drive, the driver atapicam(4) should not be used in the kernel configuration.

39.4.2. Testing the Configuration

To test the USB configuration, plug in the USB device. In the system message buffer, dmesg(8), the

drive should appear as something like:

```
umass0: USB Solid state disk, rev 1.10/1.00, addr 2
GEOM: create disk da0 dp=0xc2d74850
da0 at umass-sim0 bus 0 target 0 lun 0
da0: <Generic Traveling Disk 1.11> Removable Direct Access SCSI-2 device
da0: 1.000MB/s transfers
da0: 126MB (258048 512 byte sectors: 64H 32S/T 126C)
```

The brand, device node (da0), and other details will differ according to the device.

Since the USB device is seen as a SCSI one, `camcontrol` can be used to list the USB storage devices attached to the system:

```
# camcontrol devlist
<Generic Traveling Disk 1.11>      at scbus0 target 0 lun 0 (da0,pass0)
```

If the drive comes with a file system, it can be mounted. Refer to Adding Disks for instructions on how to format and create partitions on the USB drive.

Allowing untrusted users to mount arbitrary media, by enabling `vfs.usermount` as described below, should not be considered safe from a security point of view. Most file systems in FreeBSD were not built to safeguard against malicious devices.

To make the device mountable as a normal user, one solution is to make all users of the device a member of the `operator` group using pw(8). Next, ensure that the `operator` group is able to read and write the device by adding these lines to /etc/devfs.rules:

```
[localrules=5]
add path 'da*' mode 0660 group operator
```

If SCSI disks are installed in the system, change the second line as follows:

```
add path 'da[3-9]*' mode 0660 group operator
```

This will exclude the first three SCSI disks (da0 to da2)from belonging to the `operator` group.

Next, enable the devfs.rules(5) ruleset in /etc/rc.conf:

```
devfs_system_ruleset="localrules"
```

Next, instruct the running kernel to allow regular users to mount file systems. The easiest way is to add the following line to /etc/sysctl.conf:

```
vfs.usermount=1
```

Since this only takes effect after the next reboot use sysctl(8) to set this variable now.

The final step is to create a directory where the file system is to be mounted. This directory needs to be owned by the user that is to mount the file system. One way to do that is for `root` to create a subdirectory owned by that user as /mnt/username. In the following example, replace *username* with the login name of the user and *usergroup* with the user's primary group:

```
# mkdir /mnt/username
# chown username:usergroup /mnt/username
```

Suppose a USB thumbdrive is plugged in, and a device /dev/da0s1 appears. If the device is preformatted with a FAT file system, it can be mounted using:

```
% mount -t msdosfs -o -m=644,-M=755 /dev/da0s1 /mnt/username
```

Before the device can be unplugged, it *must* be unmounted first. After device removal, the system message buffer will show messages similar to the following:

```
umass0: at uhub0 port 1 (addr 2) disconnected
(da0:umass-sim0:0:0:0): lost device
(da0:umass-sim0:0:0:0): removing device entry
GEOM: destroy disk da0 dp=0xc2d74850
umass0: detached
```

39.4.3. Further Reading

Beside the Adding Disks and Mounting and Unmounting File Systems sections, reading various manual pages may also be useful: umass(4), camcontrol(8), and usbconfig(8) under FreeBSD 8.X or usbdevs(8) under earlier versions of FreeBSD.

39.5. Creating and Using CD Media

39.5.1. Introduction

CD media provide a number of features that differentiate them from conventional disks. Initially, they were not writable by the user. They are designed so that they can be read continuously without delays to move the head between tracks. They are also much easier to transport between systems.

CD media do have tracks, but this refers to a section of data to be read continuously and not a physical property of the disk. For example, to produce a CD on FreeBSD, prepare the data files that are going to make up the tracks on the CD, then write the tracks to the CD.

The ISO 9660 file system was designed to deal with these differences. To overcome the original file system limits, it provides an extension mechanism that allows properly written CDs to exceed those limits while still working with systems that do not support those extensions.

The sysutils/cdrtools port includes mkisofs(8), a program that can be used to produce a data file containing an ISO 9660 file system. It has options that support various extensions, and is described below.

Which tool to use to burn the CD depends on whether the CD burner is ATAPI or something else. ATAPI CD burners use `burncd` which is part of the base system. SCSI and USB CD burners should use `cdrecord` from the sysutils/cdrtools port. It is also possible to use `cdrecord` and other tools for SCSI drives on ATAPI hardware with the ATAPI/CAM module.

For CD burning software with a graphical user interface, consider X-CD-Roast or K3b. These tools are available as packages or from the sysutils/xcdroast and sysutils/k3b ports. X-CD-Roast and K3b require the ATAPI/CAM module with ATAPI hardware.

39.5.2. mkisofs

The sysutils/cdrtools port also installs mkisofs(8), which produces an ISO 9660 file system that is an image of a directory tree in the UNIX® file system name space. The simplest usage is:

```
# mkisofs -o imagefile.iso /path/to/tree
```

This command creates an *imagefile.iso* containing an ISO 9660 file system that is a copy of the tree at */path/to/tree*. In the process, it maps the file names to names that fit the limitations of the standard ISO 9660 file system, and will exclude files that have names uncharacteristic of ISO file systems.

A number of options are available to overcome these restrictions. In particular, `-R` enables the Rock Ridge extensions common to UNIX® systems, `-J` enables Joliet extensions used by Microsoft systems, and `-hfs` can be used to create HFS file systems used by Mac OS®.

For CDs that are going to be used only on FreeBSD systems, `-U` can be used to disable all filename restrictions. When used with `-R`, it produces a file system image that is identical to the specified FreeBSD tree, though it may violate the ISO 9660 standard in a number of ways.

The last option of general use is `-b`. This is used to specify the location of the boot image for use in producing an "El Torito" bootable CD. This option takes an argument which is the path to a boot image from the top of the tree being written to the CD. By default, mkisofs(8) creates an ISO image in "floppy disk emulation" mode, and thus expects the boot image to be exactly 1200, 1440 or 2880 KB in size. Some boot loaders, like the one used by the FreeBSD distribution disks, do not use emulation mode. In this case, `-no-emul-boot` should be used. So, if /tmp/myboot holds a bootable FreeBSD system with the boot image in /tmp/myboot/boot/cdboot, this command would produce the image of an ISO 9660 file system as /tmp/bootable.iso:

```
# mkisofs -R -no-emul-boot -b boot/cdboot -o /tmp/bootable.iso /tmp/myboot
```

If md is configured in the kernel, the file system can be mounted as a memory disk with:

```
# mdconfig -a -t vnode -f /tmp/bootable.iso -u 0
# mount -t cd9660 /dev/md0 /mnt
```

One can then verify that /mnt and /tmp/myboot are identical.

There are many other options available for mkisofs(8) to fine-tune its behavior. Refer to mkisofs(8) for details.

39.5.3. burncd

For an ATAPI CD burner, `burncd` can be used to burn an ISO image onto a CD. `burncd` is part of the base system, installed as /usr/sbin/burncd. Usage is very simple, as it has few options:

```
# burncd -f cddevice data imagefile.iso fixate
```

This command will burn a copy of *imagefile.iso* on *cddevice*. The default device is /dev/acd0. See burncd(8) for options to set the write speed, eject the CD after burning, and write audio data.

39.5.4. cdrecord

For systems without an ATAPI CD burner, `cdrecord` can be used to burn CDs. `cdrecord` is not part of the base system and must be installed from either the sysutils/cdrtools package or port. Changes to the base system can cause binary versions of this program to fail, possibly resulting in a "coaster". It is recommended to either upgrade the port when the system is upgraded, or for users tracking -STABLE, to upgrade the port when a new version becomes available.

While `cdrecord` has many options, basic usage is simple. Burning an ISO 9660 image is done with:

```
# cdrecord dev=device imagefile.iso
```

The tricky part of using `cdrecord` is finding the `dev` to use. To find the proper setting, use `-scanbus` which might produce results like this:

```
# cdrecord -scanbus
Cdrecord-Clone 2.01 (i386-unknown-freebsd7.0) Copyright (C) 1995-2004 J"org Schilling
Using libscg version 'schily-0.1'
scsibus0:
        0,0,0     0) 'SEAGATE ' 'ST39236LW       ' '0004' Disk
        0,1,0     1) 'SEAGATE ' 'ST39173W        ' '5958' Disk
        0,2,0     2) *
        0,3,0     3) 'iomega  ' 'jaz 1GB         ' 'J.86' Removable Disk
        0,4,0     4) 'NEC     ' 'CD-ROM DRIVE:466' '1.26' Removable CD-ROM
        0,5,0     5) *
        0,6,0     6) *
```

```
        0,7,0     7) *
scsibus1:
        1,0,0   100) *
        1,1,0   101) *
        1,2,0   102) *
        1,3,0   103) *
        1,4,0   104) *
        1,5,0   105) 'YAMAHA  ' 'CRW4260         ' '1.0q' Removable CD-ROM
        1,6,0   106) 'ARTEC   ' 'AM12S           ' '1.06' Scanner
        1,7,0   107) *
```

This lists the appropriate `dev` value for the devices on the list. Locate the CD burner, and use the three numbers separated by commas as the value for `dev`. In this case, the CRW device is 1,5,0, so the appropriate input is `dev=1,5,0`. Refer to cdrecord(1) for easier ways to specify this value and for information on writing audio tracks and controlling the write speed.

39.5.5. Duplicating Audio CDs

To duplicate an audio CD, extract the audio data from the CD to a series of files, then write these files to a blank CD. The process is slightly different for ATAPI and SCSI drives.

Procedure: SCSI Drives

1. Use `cdda2wav` to extract the audio:

   ```
   % cdda2wav -vall -D2,0 -B -Owav
   ```

2. Use `cdrecord` to write the .wav files:

   ```
   % cdrecord -v dev=2,0 -dao -useinfo  *.wav
   ```

   Make sure that *2,0* is set appropriately, as described in cdrecord.

Procedure: ATAPI Drives

With the help of the ATAPI/CAM module, `cdda2wav` can also be used on ATAPI drives. This tool is usually a better choice for most of users, as it supports jitter correction and endianness, than the method proposed below.

1. The ATAPI CD driver makes each track available as /dev/acddtnn, where *d* is the drive number, and *nn* is the track number written with two decimal digits, prefixed with zero as needed. So the first track on the first disk is /dev/acd0t01, the second is /dev/acd0t02, the third is /dev/acd0t03, and so on.

   Make sure the appropriate files exist in /dev. If the entries are missing, force the system to retaste the media:

```
# dd if=/dev/acd0 of=/dev/null count=1
```

2. Extract each track using dd(1), making sure to specify a block size when extracting the files:

```
# dd if=/dev/acd0t01 of=track1.cdr bs=2352
# dd if=/dev/acd0t02 of=track2.cdr bs=2352
...
```

3. Burn the extracted files to disk using `burncd`. Specify that these are audio files, and that `burncd` should fixate the disk when finished:

```
# burncd -f /dev/acd0 audio track1.cdr track2.cdr ... fixate
```

39.5.6. Duplicating Data CDs

It is possible to copy a data CD to an image file that is functionally equivalent to the image file created with mkisofs(8), and then use it to duplicate any data CD. The example given here assumes that the CD-ROM device is acd0. Substitute the correct CD-ROM device.

```
# dd if=/dev/acd0 of=file.iso bs=2048
```

Now that there is an image, it can be burned to CD as described above.

39.5.7. Using Data CDs

It is possible to mount and read the data on a standard data CD. By default, mount(8) assumes that a file system is of type `ufs`. Running this command:

```
# mount /dev/cd0 /mnt
```

will generate an error about `Incorrect super block`, and will fail to mount the CD. The CD does not use the `UFS` file system, so attempts to mount it as such will fail. Instead, tell mount(8) that the file system is of type `ISO9660` by specifying `-t cd9660` to mount(8). For example, to mount the CD-ROM device, /dev/cd0, under /mnt, use:

```
# mount -t cd9660 /dev/cd0 /mnt
```

Replace /dev/cd0 with the device name for the CD device. Also, `-t cd9660` executes mount_cd9660(8), meaning the above command is equivalent to:

```
# mount_cd9660 /dev/cd0 /mnt
```

While data CD-ROMs from any vendor can be mounted this way, disks with certain ISO 9660 extensions might behave oddly. For example, Joliet disks store all filenames in two-byte Unicode characters. The FreeBSD kernel does not speak Unicode, but the FreeBSD CD9660 driver is able to convert Unicode characters on the fly. If some non-English characters show up as question marks, specify the local charset with `-C`. For more information, refer to mount_cd9660(8).

In order to do this character conversion with the help of `-C`, the kernel requires the cd9660_iconv.ko module to be loaded. This can be done either by adding this line to loader.conf:

```
cd9660_iconv_load="YES"
```

and then rebooting the machine, or by directly loading the module with kldload(8).

Occasionally, `Device not configured` will be displayed when trying to mount a CD-ROM. This usually means that the CD-ROM drive thinks that there is no disk in the tray, or that the drive is not visible on the bus. It can take a couple of seconds for a CD-ROM drive to realize that a media is present, so be patient.

Sometimes, a SCSI CD-ROM may be missed because it did not have enough time to answer the bus reset. To resolve this, add the following option to the kernel configuration and rebuild the kernel.

```
options SCSI_DELAY=15000
```

This tells the SCSI bus to pause 15 seconds during boot, to give the CD-ROM drive every possible chance to answer the bus reset.

39.5.8. Burning Raw Data CDs

It is possible to burn a file directly to CD, without creating an ISO 9660 file system. Some people do this for backup purposes. This command runs more quickly than burning a standard CD:

```
# burncd -f /dev/acd1 -s 12 data archive.tar.gz fixate
```

In order to retrieve the data burned to such a CD, the data must be read from the raw device node:

```
# tar xzvf /dev/acd1
```

This type of disk can not be mounted as a normal CD-ROM and the data cannot be read under any operating system except FreeBSD. In order to mount the CD, or to share the data with another operating system, mkisofs(8) must be used as described above.

39.5.9. Using the ATAPI/CAM Driver

This driver allows ATAPI devices, such as CD/DVD drives, to be accessed through the SCSI subsystem, and so allows the use of applications like sysutils/cdrdao or cdrecord(1).

To use this driver, add the following line to /boot/loader.conf:

```
atapicam_load="YES"
```

then, reboot the system.

Users who prefer to statically compile atapicam(4) support into the kernel, should add this line to the kernel configuration file:

```
device atapicam
```

Ensure the following lines are still in the kernel configuration file:

```
device ata
device scbus
device cd
device pass
```

Then rebuild, install the new kernel, and reboot the machine.

During the boot process, the burner should show up, like so:

```
acd0: CD-RW <MATSHITA CD-RW/DVD-ROM UJDA740> at ata1-master PIO4
cd0 at ata1 bus 0 target 0 lun 0
cd0: <MATSHITA CDRW/DVD UJDA740 1.00> Removable CD-ROM SCSI-0 device
cd0: 16.000MB/s transfers
cd0: Attempt to query device size failed: NOT READY, Medium not present - tray closed
```

The drive can now be accessed via the /dev/cd0 device name. For example, to mount a CD-ROM on /mnt, type the following:

```
# mount -t cd9660 /dev/cd0 /mnt
```

As `root`, run the following command to get the SCSI address of the burner:

```
# camcontrol devlist
<MATSHITA CDRW/DVD UJDA740 1.00>   at scbus1 target 0 lun 0 (pass0,cd0)
```

In this example, `1,0,0` is the SCSI address to use with cdrecord(1) and other SCSI applications.

For more information about ATAPI/CAM and SCSI system, refer to atapicam(4) and cam(4).

39.6. Creating and Using DVD Media

39.6.1. Introduction

Compared to the CD, the DVD is the next generation of optical media storage technology. The DVD can hold more data than any CD and is the standard for video publishing.

Five physical recordable formats can be defined for a recordable DVD:

- DVD-R: This was the first DVD recordable format available. The DVD-R standard is defined by the DVD Forum. This format is write once.
- DVD-RW: This is the rewritable version of the DVD-R standard. A DVD-RW can be rewritten about 1000 times.
- DVD-RAM: This is a rewritable format which can be seen as a removable hard drive. However, this media is not compatible with most DVD-ROM drives and DVD-Video players as only a few DVD writers support the DVD-RAM format. Refer to Using a DVD-RAM for more information on DVD-RAM use.
- DVD+RW: This is a rewritable format defined by the DVD+RW Alliance. A DVD+RW can be rewritten about 1000 times.
- DVD+R: This format is the write once variation of the DVD+RW format.

A single layer recordable DVD can hold up to 4,700,000,000 bytes which is actually 4.38 GB or 4485 MB as 1 kilobyte is 1024 bytes.

A distinction must be made between the physical media and the application. For example, a DVD-Video is a specific file layout that can be written on any recordable DVD physical media such as DVD-R, DVD+R, or DVD-RW. Before choosing the type of media, ensure that both the burner and the DVD-Video player are compatible with the media under consideration.

39.6.2. Configuration

To perform DVD recording, use growisofs(1). This command is part of the sysutils/dvd+rw-tools utilities which support all DVD media types.

These tools use the SCSI subsystem to access the devices, therefore ATAPI/CAM support must be loaded or statically compiled into the kernel. This support is not needed if the burner uses the USB interface. Refer to USB Storage Devices for more details on USB device configuration.

DMA access must also be enabled for ATAPI devices, by adding the following line to /boot/loader.conf:

```
hw.ata.atapi_dma="1"
```

Before attempting to use dvd+rw-tools, consult the Hardware Compatibility Notes.

For a graphical user interface, consider using sysutils/k3b which provides a user friendly interface to growisofs(1) and many other burning tools.

39.6.3. Burning Data DVDs

Since growisofs(1) is a front-end to mkisofs, it will invoke mkisofs(8) to create the file system layout and perform the write on the DVD. This means that an image of the data does not need to be created before the burning process.

To burn to a DVD+R or a DVD-R the data in /path/to/data, use the following command:

```
# growisofs -dvd-compat -Z /dev/cd0 -J -R /path/to/data
```

In this example, `-J -R` is passed to mkisofs(8) to create an ISO 9660 file system with Joliet and Rock Ridge extensions. Refer to mkisofs(8) for more details.

For the initial session recording, `-Z` is used for both single and multiple sessions. Replace */dev/cd0*, with the name of the DVD device. Using `-dvd-compat` indicates that the disk will be closed and that the recording will be unappendable. This should also provide better media compatibility with DVD-ROM drives.

To burn a pre-mastered image, such as *imagefile.iso*, use:

```
# growisofs -dvd-compat -Z /dev/cd0=imagefile.iso
```

The write speed should be detected and automatically set according to the media and the drive being used. To force the write speed, use `-speed=`. Refer to growisofs(1) for example usage.

In order to support working files larger than 4.38GB, an UDF/ISO-9660 hybrid filesystem must be created by passing `-udf -iso-level 3` to mkisofs(8) and all related programs, such as growisofs(1). This is required only when creating an ISO image file or when writing files directly to a disk. Since a disk created this way must be mounted as an UDF filesystem with mount_udf(8), it will be usable only on an UDF aware operating system. Otherwise it will look as if it contains corrupted files.

To create this type of ISO file:

```
% mkisofs -R -J -udf -iso-level 3 -o imagefile.iso /path/to/data
```

To burn files directly to a disk:

```
# growisofs -dvd-compat -udf -iso-level 3 -Z /dev/cd0 -J -R
/path/to/data
```

When an ISO image already contains large files, no additional options are required for growisofs(1) to burn that image on a disk.

Be sure to use an up-to-date version of sysutils/cdrtools, which contains mkisofs(8), as an older version may not contain large files support. If the latest version does not work, install sysutils/cdrtools-devel and read its mkisofs(8).

39.6.4. Burning a DVD-Video

A DVD-Video is a specific file layout based on the ISO 9660 and micro-UDF (M-UDF) specifications. Since DVD-Video presents a specific data structure hierarchy, a particular program such as multimedia/dvdauthor is needed to author the DVD.

If an image of the DVD-Video file system already exists, it can be burned in the same way as any other image. If `dvdauthor` was used to make the DVD and the result is in /path/to/video, the following command should be used to burn the DVD-Video:

```
# growisofs -Z /dev/cd0 -dvd-video /path/to/video
```

`-dvd-video` is passed to mkisofs(8) to instruct it to create a DVD-Video file system layout. This option implies the `-dvd-compat` growisofs(1) option.

39.6.5. Using a DVD+RW

Unlike CD-RW, a virgin DVD+RW needs to be formatted before first use. It is *recommended* to let growisofs(1) take care of this automatically whenever appropriate. However, it is possible to use `dvd+rw-format` to format the DVD+RW:

```
# dvd+rw-format /dev/cd0
```

Only perform this operation once and keep in mind that only virgin DVD+RW medias need to be formatted. Once formatted, the DVD+RW can be burned as usual.

To burn a totally new file system and not just append some data onto a DVD+RW, the media does not need to be blanked first. Instead, write over the previous recording like this:

```
# growisofs -Z /dev/cd0 -J -R /path/to/newdata
```

The DVD+RW format supports appending data to a previous recording. This operation consists of merging a new session to the existing one as it is not considered to be multi-session writing. growisofs(1) will *grow* the ISO 9660 file system present on the media.

For example, to append data to a DVD+RW, use the following:

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

The same mkisofs(8) options used to burn the initial session should be used during next writes.

Use `-dvd-compat` for better media compatibility with DVD-ROM drives. When using DVD+RW, this option will not prevent the addition of data.

To blank the media, use:

```
# growisofs -Z /dev/cd0=/dev/zero
```

39.6.6. Using a DVD-RW

A DVD-RW accepts two disc formats: incremental sequential and restricted overwrite. By default, DVD-RW discs are in sequential format.

A virgin DVD-RW can be directly written without being formatted. However, a non-virgin DVD-RW in sequential format needs to be blanked before writing a new initial session.

To blank a DVD-RW in sequential mode:

```
# dvd+rw-format -blank=full /dev/cd0
```

A full blanking using `-blank=full` will take about one hour on a 1x media. A fast blanking can be performed using `-blank`, if the DVD-RW will be recorded in Disk-At-Once (DAO) mode. To burn the DVD-RW in DAO mode, use the command:

```
# growisofs -use-the-force-luke=dao -Z /dev/cd0=imagefile.iso
```

Since growisofs(1) automatically attempts to detect fast blanked media and engage DAO write, `-use-the-force-luke=dao` should not be required.

One should instead use restricted overwrite mode with any DVD-RW as this format is more flexible than the default of incremental sequential.

To write data on a sequential DVD-RW, use the same instructions as for the other DVD formats:

```
# growisofs -Z /dev/cd0 -J -R /path/to/data
```

To append some data to a previous recording, use `-M` with growisofs(1). However, if data is appended on a DVD-RW in incremental sequential mode, a new session will be created on the disc and the result will be a multi-session disc.

A DVD-RW in restricted overwrite format does not need to be blanked before a new initial session. Instead, overwrite the disc with `-Z`. It is also possible to grow an existing ISO 9660 file system written on the disc with `-M`. The result will be a one-session DVD.

To put a DVD-RW in restricted overwrite format, the following command must be used:

```
# dvd+rw-format /dev/cd0
```

To change back to sequential format, use:

```
# dvd+rw-format -blank=full /dev/cd0
```

39.6.7. Multi-Session

Few DVD-ROM drives support multi-session DVDs and most of the time only read the first session. DVD+R, DVD-R and DVD-RW in sequential format can accept multiple sessions. The notion of multiple sessions does not exist for the DVD+RW and the DVD-RW restricted overwrite formats.

Using the following command after an initial non-closed session on a DVD+R, DVD-R, or DVD-RW in sequential format, will add a new session to the disc:

```
# growisofs -M /dev/cd0 -J -R /path/to/nextdata
```

Using this command with a DVD+RW or a DVD-RW in restricted overwrite mode will append data while merging the new session to the existing one. The result will be a single-session disc. Use this method to add data after an initial write on these types of media.

Since some space on the media is used between each session to mark the end and start of sessions, one should add sessions with a large amount of data to optimize media space. The number of sessions is limited to 154 for a DVD+R, about 2000 for a DVD-R, and 127 for a DVD+R Double Layer.

39.6.8. For More Information

To obtain more information about a DVD, use `dvd+rw-mediainfo /dev/cd0` while the disc in the specified drive.

More information about dvd+rw-tools can be found in growisofs(1), on the dvd+rw-tools web site, and in the cdwrite mailing list archives.

When creating a problem report related to the use of dvd+rw-tools, always include the output of `dvd+rw-mediainfo`.

39.6.9. Using a DVD-RAM

39.6.9.1. Configuration

DVD-RAM writers can use either a SCSI or ATAPI interface. For ATAPI devices, DMA access has to be enabled by adding the following line to /boot/loader.conf:

```
hw.ata.atapi_dma="1"
```

39.6.9.2. Preparing the Media

A DVD-RAM can be seen as a removable hard drive. Like any other hard drive, the DVD-RAM must be formatted before it can be used. In this example, the whole disk space will be formatted with a standard UFS2 file system:

```
# dd if=/dev/zero of=/dev/acd0 bs=2k count=1
# bsdlabel -Bw acd0
# newfs /dev/acd0
```

The DVD device, acd0, must be changed according to the configuration.

39.6.9.3. Using the Media

Once the DVD-RAM has been formatted, it can be mounted as a normal hard drive:

```
# mount /dev/acd0 /mnt
```

Once mounted, the DVD-RAM will be both readable and writeable.

39.7. Creating and Using Floppy Disks

Storing data on floppy disks is sometimes useful, for example when one does not have any other removable storage media or when one needs to transfer small amounts of data to another computer.

This section explains how to use floppy disks in FreeBSD. It covers formatting and usage of 3.5inch DOS floppies, but the concepts are similar for other floppy disk formats.

39.7.1. Formatting Floppies

39.7.1.1. The Device

Floppy disks are accessed through entries in /dev, just like other devices. To access the raw floppy disk, simply use /dev/fdN.

39.7.1.2. Formatting

A floppy disk needs to be low-level formatted before it can be used. This is usually done by the vendor, but formatting is a good way to check media integrity. Although it is possible to force other disk sizes, 1440kB is what most floppy disks are designed for.

To low-level format the floppy disk, use fdformat(1). This utility expects the device name as an argument.

Make note of any error messages, as these can help determine if the disk is good or bad.

39.7.1.2.1. Formatting Floppy Disks

To format the floppy, insert a new 3.5inch floppy disk into the first floppy drive and issue:

```
# /usr/sbin/fdformat -f 1440 /dev/fd0
```

39.7.2. The Disk Label

After low-level formatting the disk, a disk label needs to placed on it. This disk label will be destroyed later, but it is needed by the system to determine the size of the disk and its geometry.

The new disk label will take over the whole disk and will contain all the proper information about the geometry of the floppy. The geometry values for the disk label are listed in /etc/disktab.

To write the disk label, use bsdlabel(8):

```
# /sbin/bsdlabel -B -w /dev/fd0 fd1440
```

39.7.3. The File System

The floppy is now ready to be high-level formatted. This will place a new file system on it so that FreeBSD can read and write to the disk. Since creating the new file system destroys the disk label, the disk label needs to be recreated whenever the disk is reformatted.

The floppy's file system can be either UFS or FAT. FAT is generally a better choice for floppies.

To put a new file system on the floppy, issue:

```
# /sbin/newfs_msdos /dev/fd0
```

The disk is now ready for use.

39.7.4. Using the Floppy

To use the floppy, mount it with mount_msdosfs(8). One can also use emulators/mtools from the Ports Collection.

39.8. Creating and Using Data Tapes

Tape technology has continued to evolve but is less likely to be used in a modern system. Modern backup systems tend to use off site combined with local removable disk drive technologies. Still, FreeBSD will support any tape drive that uses SCSI, such as LTO and older devices such as DAT. There is limited support for SATA and USB tape drives.

39.8.1. Serial Access with sa(4)

FreeBSD uses the sa(4) driver, providing /dev/sa0, /dev/nsa0, and /dev/esa0. In normal use, only /dev/sa0 is needed. /dev/nsa0 is the same physical drive as /dev/sa0 but does not rewind the tape after writing a file. This allows writing more than one file to a tape. Using /dev/esa0 ejects the tape after the device is closed, if applicable.

39.8.2. Controlling the Tape Drive with mt(1)

mt(1) is the FreeBSD utility for controlling other operations of the tape drive, such as seeking through files on a tape or writing tape control marks to the tape.

For example, the first three files on a tape can be preserved by skipping past them before writing a new file:

```
# mt -f /dev/nsa0 fsf 3
```

39.8.3. Using tar(1) to Read and Write Tape Backups

An example of writing a single file to tape using tar(1):

```
# tar cvf /dev/sa0 file
```

Recovering files from a tar(1) archive on tape into the current directory:

```
# tar xvf /dev/sa0
```

39.8.4. Using dump(8) and restore(8) to Create and Restore Backups

A simple backup of /usr with dump(8):

```
# dump -0aL -b64 -f /dev/nsa0 /usr
```

Interactively restoring files from a dump(8) file on tape into the current directory:

```
# restore -i -f /dev/nsa0
```

39.8.5. Other Tape Software

Higher-level programs are available to simplify tape backup. The most popular are Amanda and Bacula. These programs aim to make backups easier and more convenient, or to automate complex backups of multiple machines. The Ports Collection contains both these and other tape utility applications.

39.9. Backup Strategies

The first requirement in devising a backup plan is to make sure that all of the following problems are covered:

- Disk failure.
- Accidental file deletion.
- Random file corruption.
- Complete machine destruction, say by fire, including destruction of any on-site backups.

Some systems will be best served by having each of these problems covered by a completely different technique. Except for strictly personal systems with low-value data, it is unlikely that one technique will cover all of them.

Some possible techniques include:

- Archives of the whole system, backed up onto permanent, off-site media. This provides protection against all of the problems listed above, but is slow and inconvenient to restore from. Copies of the backups can be stored on site or online, but there will still be inconveniences in restoring files, especially for non-privileged users.
- Filesystem snapshots, which are really only helpful in the accidental file deletion scenario, but can be *very* helpful in that case, as well as quick and easy to deal with.
- Copies of whole file systems or disks which can be created with a periodic net/rsync of the whole machine. This is generally most useful in networks with unique requirements. For general protection against disk failure, this is usually inferior to RAID. For restoring accidentally deleted files, it can be comparable to UFS snapshots.
- RAID, which minimizes or avoids downtime when a disk fails at the expense of having to deal with disk failures more often, because there are more disks, albeit at a much lower urgency.
- Checking fingerprints of files using mtree(8). Although this is not a backup, this technique indicates when one needs to resort to backups. This is particularly important for offline backups, and should be checked periodically.

It is quite easy to come up with more techniques, many of them variations on the ones listed above. Specialized requirements usually lead to specialized techniques. For example, backing up a live database usually requires a method particular to the database software as an intermediate step. The important thing is to know which dangers should be protected against, and how each will be handled.

39.10. Backup Basics

The major backup programs built into FreeBSD are dump(8), tar(1), cpio(1), and pax(1).

39.10.1. Dump and Restore

The traditional UNIX® backup programs are `dump` and `restore`. They operate on the drive as a collection of disk blocks, below the abstractions of files, links and directories that are created by the file systems. Unlike other backup software, `dump` backs up an entire file system on a device. It is unable to backup only part of a file system or a directory tree that spans more than one file system. `dump` does not write files and directories, but rather writes the raw data blocks that comprise files and directories. When used to extract data, `restore` stores temporary files in /tmp/ by default. When using a recovery disk with a small /tmp, set `TMPDIR` to a directory with more free space in order for the restore to succeed.

If `dump` is used on the root directory, it will not back up /home, /usr or many other directories since these are typically mount points for other file systems or symbolic links into those file systems.

`dump` has quirks that remain from its early days in Version 6 of AT&T UNIX®,circa 1975. The default parameters are suitable for 9-track tapes (6250 bpi), not the high-density media available today (up to 62,182 ftpi). These defaults must be overridden on the command line to utilize the capacity of current tape drives.

It is also possible to backup data across the network to a tape drive attached to another computer with `rdump` and `rrestore`. Both programs rely upon rcmd(3) and ruserok(3) to access the remote tape drive. Therefore, the user performing the backup must be listed in .rhosts on the remote computer. The arguments to `rdump` and `rrestore` must be suitable to use on the remote computer. For example, to `rdump` from a FreeBSD computer to an Exabyte tape drive connected to a host called `komodo`, use:

```
# /sbin/rdump 0dsbfu 54000 13000 126 komodo:/dev/nsa8 /dev/da0a 2>&1
```

There are security implications to allowing .rhosts authentication, so use with caution.

It is also possible to use `dump` and `restore` in a more secure fashion over `ssh`.

Παράδειγμα 12. Using `dump` over ssh

```
# /sbin/dump -0uan -f - /usr | gzip -2 | ssh -c blowfish \
          targetuser@targetmachine.example.com dd of=/mybigfiles/dump-usr-l0.gz
```

Or, use the built-in `RSH`:

Παράδειγμα 13. Using dump over ssh with RSH Set

```
# env RSH=/usr/bin/ssh /sbin/dump -0uan -f
targetuser@targetmachine.example.com:/dev/sa0 /usr
```

39.10.2. tar

tar(1) also dates back to Version 6 of AT&T UNIX®, circa 1975. tar operates in cooperation with the file system and writes files and directories to tape. tar does not support the full range of options that are available from cpio(1), but it does not require the unusual command pipeline that cpio uses.

To tar to an Exabyte tape drive connected to a host called komodo:

```
# tar cf - . | rsh komodo dd of=tape-device obs=20b
```

When backing up over an insecure network, instead use ssh.

39.10.3. cpio

cpio(1) is the original UNIX® file interchange tape program for magnetic media. cpio includes options to perform byte-swapping, write a number of different archive formats, and pipe the data to other programs. This last feature makes cpio an excellent choice for installation media. cpio does not know how to walk the directory tree and a list of files must be provided through stdin.

Since cpio does not support backups across the network, use a pipeline and ssh to send the data to a remote tape drive.

```
# for f in directory_list; do

# find $f >> backup.list

# done
# cpio -v -o --format=newc < backup.list | ssh user@host "cat > backup_device"
```

Where *directory_list* is the list of directories to back up, *user@host* is the user/hostname combination that will be performing the backups, and *backup_device* is where the backups should be written to, such as /dev/nsa0).

39.10.4. pax

pax(1) is the IEEE/POSIX® answer to tar and cpio. Over the years the various versions of tar and cpio have become slightly incompatible. So rather than fight it out to fully standardize them, POSIX® created a new archive utility. pax attempts to read and write many of the various cpio and tar formats, plus new formats of its own. Its command set more resembles cpio than tar.

39.10.5. Amanda

Amanda (Advanced Maryland Network Disk Archiver) is a client/server backup system, rather than a single program. An Amanda server will backup to a single tape drive any number of computers that have Amanda clients and a network connection to the Amanda server. A common problem at sites with a number of large disks is that the length of time required to backup to data directly to tape exceeds the amount of time available for the task. Amanda solves this problem by using a "holding disk" to backup several file systems at the same time. Amanda creates "archive sets": a group of tapes used over a period of time to create full backups of all the file systems listed in Amanda's configuration file. The "archive set" also contains nightly incremental, or differential, backups of all the file systems. Restoring a damaged file system requires the most recent full backup and the incremental backups.

The configuration file provides fine grained control of backups and the network traffic that Amanda generates. Amanda will use any of the above backup programs to write the data to tape. Amanda is not installed by but is available as either a port or package.

39.10.6. Do Nothing

"Do nothing" is not a computer program, but it is the most widely used backup strategy. There are no initial costs. There is no backup schedule to follow. Just say no. If something happens to your data, grin and bear it!

If your time and data is worth little to nothing, then "Do nothing" is the most suitable backup program for the computer. But beware, FreeBSD is a useful tool and over time it can be used to create a valuable collection of files.

"Do nothing" is the correct backup method for /usr/obj and other directory trees that can be exactly recreated by the computer. An example is the files that comprise the HTML or PostScript® version of this Handbook. These document formats have been created from XML input files. Creating backups of the HTML or PostScript® files is not necessary if the XML files are backed up regularly.

39.10.7. Which Backup Program Is Best?

dump(8) *Period.* Elizabeth D. Zwicky torture tested all the backup programs discussed here. The clear choice for preserving all your data and all the peculiarities of UNIX® file systems is `dump`. Elizabeth created file systems containing a large variety of unusual conditions (and some not so unusual ones) and tested each program by doing a backup and restore of those file systems. The peculiarities included: files with holes, files with holes and a block of nulls, files with funny characters in their names, unreadable and unwritable files, devices, files that change size during the backup, files that are created/deleted during the backup and more. She presented the results at LISA V in Oct. 1991. See torture-testing Backup and Archive Programs.

39.10.8. Emergency Restore Procedure

39.10.8.1. Before the Disaster

There are four steps which should be performed in preparation for any disaster that may occur.

First, print the bsdlabel of each disk using a command such as `bsdlabel da0 | lpr`. Also print a copy of /etc/fstab and all boot messages.

Second, burn a "livefs" CD. This CD contains support for booting into a FreeBSD "livefs" rescue mode, allowing the user to perform many tasks like running dump(8), restore(8), fdisk(8), bsdlabel(8), newfs(8), mount(8), and more. The livefs CD image for FreeBSD/i386 11.2-RELEASE is available from ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/ISO-IMAGES/11.2/FreeBSD-11.2-RELEASE-i386-livefs.iso.

Livefs CD images are not available for FreeBSD 12.0-RELEASE and later. In addition to the CD-ROM installation images, flash drive installation images may be used to recover a system. The "memstick" image for FreeBSD/i386 12.0-RELEASE is available from ftp://ftp.FreeBSD.org/pub/FreeBSD/releases/i386/i386/ISO-IMAGES/12.0/FreeBSD-12.0-RELEASE-i386-memstick.img.

Third, create backup tapes regularly. Any changes that made after the last backup may be irretrievably lost. Write-protect the backup media.

Fourth, test the "livefs" CD and the backups. Make notes of the procedure. Store these notes with the CD, the printouts, and the backups. These notes may prevent the inadvertent destruction of the backups while under the stress of performing an emergency recovery.

For an added measure of security, store an extra "livefs" CD and the latest backup at a remote location, where a remote location is *not* the basement of the same building. A remote location should be physically separated from the computers and disk drives by a significant distance.

39.10.8.2. After the Disaster

First, determine if the hardware survived. Thanks to regular, off-site backups, there is no need to worry about the software.

If the hardware has been damaged, the parts should be replaced before attempting to use the computer.

If the hardware is okay, insert the "livefs" CD and boot the computer. The original install menu will be displayed on the screen. Select the correct country, then choose Fixit — Repair mode with CD-ROM/DVD/floppy or start a shell. then select CD-ROM/DVD — Use the live filesystem CD-ROM/DVD. `restore` and the other needed programs are located in /mnt2/rescue.

Recover each file system separately.

Try to `mount` the root partition of the first disk using `mount /dev/da0a /mnt`. If the bsdlabel was damaged, use `bsdlabel` to re-partition and label the disk to match the label that was printed and saved. Use `newfs` to re-create the file systems. Re-mount the root partition of the disk read-write using `mount -u -o rw /mnt`. Use the backups to recover the data for this file system. Unmount the file system with `umount /mnt`. Repeat for each file system that was damaged.

Once the system is running, backup the data onto new media as whatever caused the crash or data loss may strike again. Another hour spent now may save further distress later.

39.11. Network, Memory, and File-Backed File Systems

In addition to physical disks such as floppies, CDs, and hard drives, FreeBSD also supports *virtual disks*.

These include network file systems such as the Network File System and Coda, memory-based file systems, and file-backed file systems.

According to the FreeBSD version, the tools used for the creation and use of file-backed and memory-based file systems differ.

Use devfs(5) to allocate device nodes transparently for the user.

39.11.1. File-Backed File System

mdconfig(8) is used to configure and enable memory disks, md(4), under FreeBSD. To use mdconfig(8), md(4) must be first loaded. When using a custom kernel configuration file, ensure it includes this line:

```
device md
```

mdconfig(8) supports several types of memory backed virtual disks: memory disks allocated with malloc(9) and memory disks using a file or swap space as backing. One possible use is the mounting of CD images.

To mount an existing file system image:

Παράδειγμα 14. Using `mdconfig` to Mount an Existing File System Image

```
# mdconfig -a -t vnode -f diskimage -u 0
# mount /dev/md0 /mnt
```

To create a new file system image with mdconfig(8):

Παράδειγμα 15. Creating a New File-Backed Disk with `mdconfig`

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdconfig -a -t vnode -f newimage -u 0
# bsdlabel -w md0 auto
# newfs md0a
/dev/md0a: 5.0MB (10224 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 1.25MB, 80 blks, 192 inodes.
super-block backups (for fsck -b #) at:
 160, 2720, 5280, 7840
```

```
# mount /dev/md0a /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0a       4710    4  4330     0%    /mnt
```

If unit number is not specified with `-u`, mdconfig(8) uses the md(4) automatic allocation to select an unused device. The name of the allocated unit will be output to stdout, such as md4. Refer to mdconfig(8) for more details about.

While mdconfig(8) is useful, it takes several command lines to create a file-backed file system. FreeBSD also comes with mdmfs(8) which automatically configures a md(4) disk using mdconfig(8), puts a UFS file system on it using newfs(8), and mounts it using mount(8). For example, to create and mount the same file system image as above, type the following:

Παράδειγμα 16. Configure and Mount a File-Backed Disk with `mdmfs`

```
# dd if=/dev/zero of=newimage bs=1k count=5k
5120+0 records in
5120+0 records out
# mdmfs -F newimage -s 5m md0 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md0        4718    4  4338     0%    /mnt
```

When `md` is used without a unit number, mdmfs(8) uses the md(4) auto-unit feature to automatically select an unused device. For more details about mdmfs(8), refer to its manual page.

39.11.2. Memory-Based File System

For a memory-based file system, "swap backing" should normally be used. This does not mean that the memory disk will be swapped out to disk by default, but rather that the memory disk will be allocated from a memory pool which can be swapped out to disk if needed. It is also possible to create memory-based disks which are malloc(9) backed, but using large malloc backed memory disks can result in a system panic if the kernel runs out of memory.

Παράδειγμα 17. Creating a New Memory-Based Disk with `mdconfig`

```
# mdconfig -a -t swap -s 5m -u 1
# newfs -U md1
/dev/md1: 5.0MB (10240 sectors) block size 16384, fragment size 2048
        using 4 cylinder groups of 1.27MB, 81 blks, 192 inodes.
        with soft updates
super-block backups (for fsck -b #) at:
 160, 2752, 5344, 7936
# mount /dev/md1 /mnt
# df /mnt
```

```
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md1        4718    4  4338     0%    /mnt
```

Παράδειγμα 18. Creating a New Memory-Based Disk with `mdmfs`

```
# mdmfs -s 5m md2 /mnt
# df /mnt
Filesystem 1K-blocks Used Avail Capacity  Mounted on
/dev/md2        4846    2  4458     0%    /mnt
```

39.11.3. Detaching a Memory Disk from the System

When a memory-based or file-based file system is no longer in use, its resources should be released back to the system. First, unmount the file system, then use mdconfig(8) to detach the disk from the system and release the resources.

For example, to detach and free all resources used by /dev/md4:

```
# mdconfig -d -u 4
```

It is possible to list information about configured md(4) devices by running `mdconfig -l`.

39.12. File System Snapshots

FreeBSD offers a feature in conjunction with Soft Updates: file system snapshots.

UFS snapshots allow a user to create images of specified file systems, and treat them as a file. Snapshot files must be created in the file system that the action is performed on, and a user may create no more than 20 snapshots per file system. Active snapshots are recorded in the superblock so they are persistent across unmount and remount operations along with system reboots. When a snapshot is no longer required, it can be removed using rm(1). While snapshots may be removed in any order, all the used space may not be acquired because another snapshot will possibly claim some of the released blocks.

The un-alterable `snapshot` file flag is set by mksnap_ffs(8) after initial creation of a snapshot file. unlink(1) makes an exception for snapshot files since it allows them to be removed.

Snapshots are created using mount(8). To place a snapshot of /var in the file /var/snapshot/snap, use the following command:

```
# mount -u -o snapshot /var/snapshot/snap /var
```

Alternatively, use mksnap_ffs(8) to create the snapshot:

```
# mksnap_ffs /var /var/snapshot/snap
```

One can find snapshot files on a file system, such as /var, using find(1):

```
# find /var -flags snapshot
```

Once a snapshot has been created, it has several uses:

- Some administrators will use a snapshot file for backup purposes, because the snapshot can be transferred to CDs or tape.
- The file system integrity checker, fsck(8), may be run on the snapshot. Assuming that the file system was clean when it was mounted, this should always provide a clean and unchanging result.
- Running dump(8) on the snapshot will produce a dump file that is consistent with the file system and the timestamp of the snapshot. dump(8) can also take a snapshot, create a dump image, and then remove the snapshot in one command by using `-L`.
- The snapshot can be mounted as a frozen image of the file system. To mount(8) the snapshot /var/snapshot/snap run:

  ```
  # mdconfig -a -t vnode -f /var/snapshot/snap -u 4
  # mount -r /dev/md4 /mnt
  ```

The frozen /var is now available through /mnt. Everything will initially be in the same state it was during the snapshot creation time. The only exception is that any earlier snapshots will appear as zero length files. To unmount the snapshot, use:

```
# umount /mnt
# mdconfig -d -u 4
```

For more information about `softupdates` and file system snapshots, including technical papers, visit Marshall Kirk McKusick's website at http://www.mckusick.com/.

39.13. File System Quotas

Quotas are an optional feature of the operating system that can be used to limit the amount of disk space or the number of files a user or members of a group may allocate on a per-file system basis. This is used most often on timesharing systems where it is desirable to limit the amount of resources any one user or group of users may allocate. This prevents one user or group of users from consuming all of the available disk space.

39.13.1. Configuring the System to Enable Disk Quotas

Before using disk quotas, quota support must be added to the kernel by adding the following line to

the kernel configuration file:

```
options QUOTA
```

Before FreeBSD 9.2, the GENERIC kernel usually did not include this option. `sysctl kern.features.ufs_quota` can be used to test whether the current kernel supports quotas. If the option is not present, a custom kernel must be compiled. Refer to Configuring the FreeBSD Kernel for more information on kernel configuration.

Next, enable disk quotas in /etc/rc.conf:

```
quota_enable="YES"
```

For finer control over quota startup, an additional configuration variable is available. Normally on bootup, the quota integrity of each file system is checked by quotacheck(8). This program insures that the data in the quota database properly reflects the data on the file system. This is a time consuming process that will significantly affect the time the system takes to boot. To skip this step, add this variable to /etc/rc.conf:

```
check_quotas="NO"
```

Finally, edit /etc/fstab to enable disk quotas on a per-file system basis. This is when user or group quotas can be enabled on the file systems.

To enable per-user quotas on a file system, add `userquota` to the options field in the /etc/fstab entry for the file system to enable quotas on. For example:

```
/dev/da1s2g   /home    ufs rw,userquota 1 2
```

To enable group quotas, instead use `groupquota`. To enable both user and group quotas, change the entry as follows:

```
/dev/da1s2g    /home    ufs rw,userquota,groupquota 1 2
```

By default, the quota files are stored in the root directory of the file system as quota.user and quota.group. Refer to fstab(5) for more information. Even though an alternate location for the quota files can be specified, this is not recommended because the various quota utilities do not seem to handle this properly.

Once the configuration is complete, reboot the system with the new kernel. /etc/rc will automatically run the appropriate commands to create the initial quota files for all of the quotas enabled in /etc/fstab. There is no need to manually create any zero length quota files.

In the normal course of operations, there should be no need to manually run quotacheck(8),

quotaon(8), or quotaoff(8). However, one should read their manual pages to be familiar with their operation.

39.13.2. Setting Quota Limits

Once the system has been configured to enable quotas, verify they really are enabled by running:

```
# quota -v
```

There should be a one line summary of disk usage and current quota limits for each file system that quotas are enabled on.

The system is now ready to be assigned quota limits with edquota(8).

Several options are available to enforce limits on the amount of disk space a user or group may allocate, and how many files they may create. Allocations can be limited based on disk space (block quotas), number of files (inode quotas), or a combination of both. Each limits is further broken down into two categories: hard and soft limits.

A hard limit may not be exceeded. Once a user reaches a hard limit, no further allocations can be made on that file system by that user. For example, if the user has a hard limit of 500 kbytes on a file system and is currently using 490 kbytes, the user can only allocate an additional 10 kbytes. Attempting to allocate an additional 11 kbytes will fail.

Soft limits can be exceeded for a limited amount of time, known as the grace period, which is one week by default. If a user stays over their limit longer than the grace period, the soft limit turns into a hard limit and no further allocations are allowed. When the user drops back below the soft limit, the grace period is reset.

The following is an example output from edquota(8). When edquota(8) is invoked, the editor specified by `EDITOR` is opened in order to edit the quota limits. The default editor is set to vi.

```
# edquota -u test
```

```
Quotas for user test:
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
        inodes in use: 7, limits (soft = 50, hard = 60)
/usr/var: kbytes in use: 0, limits (soft = 50, hard = 75)
        inodes in use: 0, limits (soft = 50, hard = 60)
```

There are normally two lines for each file system that has quotas enabled. One line represents the block limits and the other represents the inode limits. Change the value to modify the quota limit. For example, to raise this user's block limit from a soft limit of 50 and a hard limit of 75 to a soft limit of 500 and a hard limit of 600, change:

```
/usr: kbytes in use: 65, limits (soft = 50, hard = 75)
```

to:

```
/usr: kbytes in use: 65, limits (soft = 500, hard = 600)
```

The new quota limits take affect upon exiting the editor.

Sometimes it is desirable to set quota limits on a range of UIDs. This can be done by passing `-p` to edquota(8). First, assign the desired quota limit to a user, then run `edquota -p protouser startuid-enduid`. For example, if `test` has the desired quota limits, the following command will duplicate those quota limits for UIDs 10,000 through 19,999:

```
# edquota -p test 10000-19999
```

For more information, refer to edquota(8).

39.13.3. Checking Quota Limits and Disk Usage

Either quota(1) or repquota(8) can be used to check quota limits and disk usage. To check individual user or group quotas and disk usage, use quota(1). A user may only examine their own quota and the quota of a group they are a member of. Only the superuser may view all user and group quotas. To get a summary of all quotas and disk usage for file systems with quotas enabled, use repquota(8).

The following is sample output from `quota -v` for a user that has quota limits on two file systems.

```
Disk quotas for user test (uid 1002):
     Filesystem  usage    quota   limit   grace   files   quota   limit   grace
           /usr      65*     50      75   5days       7      50      60
       /usr/var       0      50      75               0      50      60
```

In this example, the user is currently 15 kbytes over the soft limit of 50 kbytes on /usr and has 5 days of grace period left. The asterisk * indicates that the user is currently over the quota limit.

Normally, file systems that the user is not using any disk space on will not show in the output of quota(1), even if the user has a quota limit assigned for that file system. Use `-v` to display those file systems, such as /usr/var in the above example.

39.13.4. Quotas over NFS

Quotas are enforced by the quota subsystem on the NFS server. The rpc.rquotad(8) daemon makes quota information available to quota(1) on NFS clients, allowing users on those machines to see their quota statistics.

Enable `rpc.rquotad` in /etc/inetd.conf like so:

```
rquotad/1      dgram rpc/udp wait root /usr/libexec/rpc.rquotad rpc.rquotad
```

Now restart `inetd`:

```
# service inetd restart
```

39.14. Encrypting Disk Partitions

FreeBSD offers excellent online protections against unauthorized data access. File permissions and Mandatory Access Control (MAC) help prevent unauthorized users from accessing data while the operating system is active and the computer is powered up. However, the permissions enforced by the operating system are irrelevant if an attacker has physical access to a computer and can move the computer's hard drive to another system to copy and analyze the data.

Regardless of how an attacker may have come into possession of a hard drive or powered-down computer, both the GEOM Based Disk Encryption (`gbde`) and `geli` cryptographic subsystems in FreeBSD are able to protect the data on the computer's file systems against even highly-motivated attackers with significant resources. Unlike cumbersome encryption methods that encrypt only individual files, `gbde` and `geli` transparently encrypt entire file systems. No cleartext ever touches the hard drive's platter.

39.14.1. Disk Encryption with gbde

1. Configuring gbde requires superuser privileges.

   ```
   % su -
   Password:
   ```

2. If using a custom kernel configuration file, ensure it contains this line:

   ```
   options GEOM_BDE
   ```

   If the kernel already contains this support, use `kldload` to load gbde(4):

   ```
   # kldload geom_bde
   ```

39.14.1.1. Preparing the Encrypted Hard Drive

The following example demonstrates adding a new hard drive to a system that will hold a single encrypted partition. This partition will be mounted as /private. gbde can also be used to encrypt /home and /var/mail, but this requires more complex instructions which exceed the scope of this introduction.

1. Add the New Hard Drive

   Install the new drive to the system as explained in Adding Disks. For the purposes of this example, a new hard drive partition has been added as /dev/ad4s1c and /dev/ad0s1* represents the existing standard FreeBSD partitions.

   ```
   # ls /dev/ad*
   /dev/ad0        /dev/ad0s1b     /dev/ad0s1e     /dev/ad4s1
   /dev/ad0s1      /dev/ad0s1c     /dev/ad0s1f     /dev/ad4s1c
   /dev/ad0s1a     /dev/ad0s1d     /dev/ad4
   ```

2. Create a Directory to Hold gbde Lock Files

   ```
   # mkdir /etc/gbde
   ```

   The gbde lock file contains information that gbde requires to access encrypted partitions. Without access to the lock file, gbde will not be able to decrypt the data contained in the encrypted partition without significant manual intervention which is not supported by the software. Each encrypted partition uses a separate lock file.

3. Initialize the gbde Partition

   A gbde partition must be initialized before it can be used. This initialization needs to be performed only once:

   ```
   # gbde init /dev/ad4s1c -i -L /etc/gbde/ad4s1c.lock
   ```

   gbde(8) will open the default editor, in order to set various configuration options in a template. For use with UFS1 or UFS2, set the sector_size to 2048:

   ```
   # $FreeBSD: src/sbin/gbde/template.txt,v 1.1.36.1 2009/08/03 08:13:06 kensmith Exp
   $
   #
   # Sector size is the smallest unit of data which can be read or written.
   # Making it too small decreases performance and decreases available space.
   # Making it too large may prevent filesystems from working.  512 is the
   # minimum and always safe.  For UFS, use the fragment size
   #
   sector_size =   2048
   [...]
   ```

   gbde(8) will ask the user twice to type the passphrase used to secure the data. The passphrase must be the same both times. The ability of gbde to protect data depends entirely on the quality of the passphrase. For tips on how to select a secure passphrase that is easy to remember, see the Diceware Passphrase website.

`gbde init` creates a lock file for the gbde partition. In this example, it is stored as /etc/gbde/ad4s1c.lock. gbde lock files must end in ".lock" in order to be correctly detected by the /etc/rc.d/gbde start up script.

gbde lock files *must* be backed up together with the contents of any encrypted partitions. While deleting a lock file alone cannot prevent a determined attacker from decrypting a gbde partition, without the lock file, the legitimate owner will be unable to access the data on the encrypted partition without a significant amount of work that is totally unsupported by gbde(8).

4. Attach the Encrypted Partition to the Kernel

```
# gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c.lock
```

This command will prompt to input the passphrase that was selected during the initialization of the encrypted partition. The new encrypted device will appear in /dev as /dev/device_name.bde:

```
# ls /dev/ad*
/dev/ad0        /dev/ad0s1b     /dev/ad0s1e     /dev/ad4s1
/dev/ad0s1      /dev/ad0s1c     /dev/ad0s1f     /dev/ad4s1c
/dev/ad0s1a     /dev/ad0s1d     /dev/ad4        /dev/ad4s1c.bde
```

5. Create a File System on the Encrypted Device

Once the encrypted device has been attached to the kernel, a file system can be created on the device using newfs(8). This example creates a UFS2 file system with soft updates enabled.

```
# newfs -U /dev/ad4s1c.bde
```

newfs(8) must be performed on an attached gbde partition which is identified by a *.bde extension to the device name.

6. Mount the Encrypted Partition

Create a mount point for the encrypted file system:

```
# mkdir /private
```

Mount the encrypted file system:

```
# mount /dev/ad4s1c.bde /private
```

7. Verify That the Encrypted File System is Available

The encrypted file system should now be visible to df(1) and be available for use.

```
% df -H
Filesystem         Size   Used  Avail Capacity  Mounted on
/dev/ad0s1a       1037M    72M   883M     8%    /
/devfs             1.0K   1.0K     0B   100%    /dev
/dev/ad0s1f        8.1G    55K   7.5G     0%    /home
/dev/ad0s1e       1037M   1.1M   953M     0%    /tmp
/dev/ad0s1d        6.1G   1.9G   3.7G    35%    /usr
/dev/ad4s1c.bde    150G   4.1K   138G     0%    /private
```

39.14.1.2. Mounting Existing Encrypted File Systems

After each boot, any encrypted file systems must be re-attached to the kernel, checked for errors, and mounted, before the file systems can be used. The required commands must be executed as `root`.

1. Attach the `gbde` Partition to the Kernel

   ```
   # gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c.lock
   ```

   This command will prompt for the passphrase that was selected during initialization of the encrypted gbde partition.

2. Check the File System for Errors

   Since encrypted file systems cannot yet be listed in /etc/fstab for automatic mounting, the file systems must be checked for errors by running fsck(8) manually before mounting:

   ```
   # fsck -p -t ffs /dev/ad4s1c.bde
   ```

3. Mount the Encrypted File System

   ```
   # mount /dev/ad4s1c.bde /private
   ```

   The encrypted file system is now available for use.

39.14.1.2.1. Automatically Mounting Encrypted Partitions

It is possible to create a script to automatically attach, check, and mount an encrypted partition, but for security reasons the script should not contain the gbde(8) password. Instead, it is recommended that such scripts be run manually while providing the password via the console or ssh(1).

As an alternative, an rc.d script is provided. Arguments for this script can be passed via rc.conf(5):

```
gbde_autoattach_all="YES"
```

```
gbde_devices="ad4s1c"
gbde_lockdir="/etc/gbde"
```

This requires that the gbde passphrase be entered at boot time. After typing the correct passphrase, the gbde encrypted partition will be mounted automatically. This can be useful when using gbde on laptops.

39.14.1.3. Cryptographic Protections Employed by `gbde`

gbde(8) encrypts the sector payload using 128-bit AES in CBC mode. Each sector on the disk is encrypted with a different AES key. For more information on the cryptographic design, including how the sector keys are derived from the user-supplied passphrase, refer to gbde(4).

39.14.1.4. Compatibility Issues

sysinstall(8) is incompatible with gbde-encrypted devices. All *.bde devices must be detached from the kernel before starting sysinstall(8) or it will crash during its initial probing for devices. To detach the encrypted device used in the example, use the following command:

```
# gbde detach /dev/ad4s1c
```

39.14.2. Disk Encryption with `geli`

An alternative cryptographic GEOM class is available through geli(8). `geli` differs from `gbde`; offers different features, and uses a different scheme for doing cryptographic work.

geli(8) provides the following features:

- Utilizes the crypto(9) framework and, when cryptographic hardware is available, `geli` uses it automatically.
- Supports multiple cryptographic algorithms such as AES, Blowfish, and 3DES.
- Allows the root partition to be encrypted. The passphrase used to access the encrypted root partition will be requested during system boot.
- Allows the use of two independent keys such as a "key" and a "company key".
- `geli` is fast as it performs simple sector-to-sector encryption.
- Allows backup and restore of master keys. If a user destroys their keys, it is still possible to get access to the data by restoring keys from the backup.
- Allows a disk to attach with a random, one-time key which is useful for swap partitions and temporary file systems.

More `geli` features can be found in geli(8).

This section describes how to enable support for `geli` in the FreeBSD kernel and explains how to create and use a `geli` encryption provider.

Superuser privileges are required since modifications to the kernel are necessary.

1. Adding `geli` Support to the Kernel

   For a custom kernel, ensure the kernel configuration file contains these lines:

   ```
   options GEOM_ELI
   device crypto
   ```

   Alternatively, the `geli` module can be loaded at boot time by adding the following line to /boot/loader.conf:

   ```
   geom_eli_load="YES"
   ```

   geli(8) should now be supported by the kernel.

2. Generating the Master Key

   The following example describes how to generate a key file which will be used as part of the master key for the encrypted provider mounted under /private. The key file will provide some random data used to encrypt the master key. The master key will also be protected by a passphrase. The provider's sector size will be 4kB. The example will describe how to attach to the `geli` provider, create a file system on it, mount it, work with it, and finally, how to detach it.

   It is recommended to use a bigger sector size, such as 4kB, for better performance.

   The master key will be protected with a passphrase and the data source for the key file will be /dev/random. The sector size of the provider /dev/da2.eli will be 4kB.

   ```
   # dd if=/dev/random of=/root/da2.key bs=64 count=1
   # geli init -s 4096 -K /root/da2.key /dev/da2
   Enter new passphrase:
   Reenter new passphrase:
   ```

   It is not mandatory to use both a passphrase and a key file as either method of securing the master key can be used in isolation.

   If the key file is given as "-", standard input will be used. This example shows how more than one key file can be used:

   ```
   # cat keyfile1 keyfile2 keyfile3 | geli init -K - /dev/da2
   ```

3. Attaching the Provider with the Generated Key

   ```
   # geli attach -k /root/da2.key /dev/da2
   Enter passphrase:
   ```

The new plaintext device will be named /dev/da2.eli.

```
# ls /dev/da2*
/dev/da2  /dev/da2.eli
```

4. Creating the New File System

```
# dd if=/dev/random of=/dev/da2.eli bs=1m
# newfs /dev/da2.eli
# mount /dev/da2.eli /private
```

The encrypted file system should now be visible to df(1) and be available for use:

```
# df -H
Filesystem     Size   Used  Avail Capacity  Mounted on
/dev/ad0s1a    248M    89M   139M    38%    /
/devfs         1.0K   1.0K     0B   100%    /dev
/dev/ad0s1f    7.7G   2.3G   4.9G    32%    /usr
/dev/ad0s1d    989M   1.5M   909M     0%    /tmp
/dev/ad0s1e    3.9G   1.3G   2.3G    35%    /var
/dev/da2.eli   150G   4.1K   138G     0%    /private
```

5. Unmounting and Detaching the Provider

Once the work on the encrypted partition is done, and the /private partition is no longer needed, it is prudent to consider unmounting and detaching the `geli` encrypted partition from the kernel:

```
# umount /private
# geli detach da2.eli
```

More information about the use of geli(8) can be found in its manual page.

39.14.2.1. Using the geli rc.d Script

`geli` comes with a rc.d script which can be used to simplify the usage of `geli`. An example of configuring `geli` through rc.conf(5) follows:

```
geli_devices="da2"
geli_da2_flags="-p -k /root/da2.key"
```

This configures /dev/da2 as a `geli` provider of which the master key file is located in /root/da2.key. `geli` will not use a passphrase when attaching to the provider if `-P` was given during the `geli init` phase. The system will detach the `geli` provider from the kernel before the system shuts down.

More information about configuring rc.d is provided in the rc.d section of the Handbook.

39.15. Encrypting Swap Space

Like the encryption of disk partitions, encryption of swap space is used to protect sensitive information. Consider an application that deals with passwords. As long as these passwords stay in physical memory, these passwords will not be written to disk and be cleared after a reboot. If FreeBSD starts swapping out memory pages to free space for other applications, the passwords may be written to the disk platters unencrypted. Encrypting swap space can be a solution for this scenario.

The gbde(8) or geli(8) encryption systems may be used for swap encryption. Both systems use the encswap rc.d script.

For the remainder of this section, ad0s1b will be the swap partition.

Swap partitions are not encrypted by default and should be cleared of any sensitive data before continuing. To overwrite the current swap parition with random garbage, execute the following command:

```
# dd if=/dev/random of=/dev/ad0s1b bs=1m
```

39.15.1. Swap Encryption with gbde(8)

The `.bde` suffix should be added to the device in the respective /etc/fstab swap line:

```
# Device        Mountpoint  FStype  Options     Dump    Pass#
/dev/ad0s1b.bde     none        swap    sw      0   0
```

39.15.2. Swap Encryption with geli(8)

The procedure for instead using geli(8) for swap encryption is similar to that of using gbde(8). The `.eli` suffix should be added to the device in the respective /etc/fstab swap line:

```
# Device        Mountpoint  FStype  Options     Dump    Pass#
/dev/ad0s1b.eli     none        swap    sw      0   0
```

geli(8) uses the AES algorithm with a key length of 128 bit by default. These defaults can be altered by using `geli_swap_flags` in /etc/rc.conf. The following line tells the encswap rc.d script to create geli(8) swap partitions using the Blowfish algorithm with a key length of 128 bits and a sectorsize of 4 kilobytes, and sets "detach on last close":

```
geli_swap_flags="-e blowfish -l 128 -s 4096 -d"
```

Refer to the description of `onetime` in geli(8) for a list of possible options.

39.15.3. Encrypted Swap Verification

Once the system has rebooted, proper operation of the encrypted swap can be verified using `swapinfo`.

If gbde(8) is being used:

```
% swapinfo
Device          1K-blocks     Used    Avail Capacity
/dev/ad0s1b.bde    542720        0   542720     0%
```

If geli(8) is being used:

```
% swapinfo
Device          1K-blocks     Used    Avail Capacity
/dev/ad0s1b.eli    542720        0   542720     0%
```

39.16. Highly Available Storage (HAST)

39.16.1. Synopsis

High availability is one of the main requirements in serious business applications and highly-available storage is a key component in such environments. Highly Available STorage, or HAST, was developed by Paweł Jakub Dawidek <pjd@FreeBSD.org> as a framework which allows transparent storage of the same data across several physically separated machines connected by a TCP/IP network. HAST can be understood as a network-based RAID1 (mirror), and is similar to the DRBD® storage system known from the GNU/Linux® platform. In combination with other high-availability features of FreeBSD like CARP, HAST makes it possible to build a highly-available storage cluster that is resistant to hardware failures.

After reading this section, you will know:

- What HAST is, how it works and which features it provides.
- How to set up and use HAST on FreeBSD.
- How to integrate CARP and devd(8) to build a robust storage system.

Before reading this section, you should:

- Understand UNIX® and FreeBSD Basics.
- Know how to configure network interfaces and other core FreeBSD subsystems.
- Have a good understanding of FreeBSD networking.

The HAST project was sponsored by The FreeBSD Foundation with support from OMCnet Internet Service GmbH and TransIP BV.

39.16.2. HAST Features

The main features of the HAST system are:

- Can be used to mask I/O errors on local hard drives.
- File system agnostic as it works with any file system supported by FreeBSD.
- Efficient and quick resynchronization, synchronizing only blocks that were modified during the downtime of a node.
- Can be used in an already deployed environment to add additional redundancy.
- Together with CARP, Heartbeat, or other tools, it can be used to build a robust and durable storage system.

39.16.3. HAST Operation

As HAST provides a synchronous block-level replication of any storage media to several machines, it requires at least two physical machines: the `primary`, also known as the `master` node, and the `secondary` or `slave` node. These two machines together are referred to as a cluster.

HAST is currently limited to two cluster nodes in total.

Since HAST works in a primary-secondary configuration, it allows only one of the cluster nodes to be active at any given time. The `primary` node, also called `active`, is the one which will handle all the I/O requests to HAST-managed devices. The `secondary` node is automatically synchronized from the `primary` node.

The physical components of the HAST system are:

- local disk on primary node, and
- disk on remote, secondary node.

HAST operates synchronously on a block level, making it transparent to file systems and applications. HAST provides regular GEOM providers in /dev/hast/ for use by other tools or applications, thus there is no difference between using HAST-provided devices and raw disks or partitions.

Each write, delete, or flush operation is sent to the local disk and to the remote disk over TCP/IP. Each read operation is served from the local disk, unless the local disk is not up-to-date or an I/O error occurs. In such case, the read operation is sent to the secondary node.

39.16.3.1. Synchronization and Replication Modes

HAST tries to provide fast failure recovery. For this reason, it is very important to reduce synchronization time after a node's outage. To provide fast synchronization, HAST manages an on-disk bitmap of dirty extents and only synchronizes those during a regular synchronization, with an exception of the initial sync.

There are many ways to handle synchronization. HAST implements several replication modes to handle different synchronization methods:

- *memsync*: report write operation as completed when the local write operation is finished and when the remote node acknowledges data arrival, but before actually storing the data. The data on the remote node will be stored directly after sending the acknowledgement. This mode is intended to reduce latency, but still provides very good reliability.
- *fullsync*: report write operation as completed when local write completes and when remote write completes. This is the safest and the slowest replication mode. This mode is the default.
- *async*: report write operation as completed when local write completes. This is the fastest and the most dangerous replication mode. It should be used when replicating to a distant node where latency is too high for other modes.

39.16.4. HAST Configuration

HAST requires `GEOM_GATE` support which is not present in the default `GENERIC` kernel. However, the `geom_gate.ko` loadable module is available in the default FreeBSD installation. Alternatively, to build `GEOM_GATE` support into the kernel statically, add this line to the custom kernel configuration file:

```
options GEOM_GATE
```

The HAST framework consists of several parts from the operating system's point of view:

- the hastd(8) daemon responsible for data synchronization,
- the hastctl(8) userland management utility,
- and the hast.conf(5) configuration file.

The following example describes how to configure two nodes in `master-slave` / `primary-secondary` operation using HAST to replicate the data between the two. The nodes will be called `hasta` with an IP address of *172.16.0.1* and `hastb` with an IP of address *172.16.0.2*. Both nodes will have a dedicated hard drive /dev/ad6 of the same size for HAST operation. The HAST pool, sometimes also referred to as a resource or the GEOM provider in /dev/hast/, will be called test.

Configuration of HAST is done using /etc/hast.conf. This file should be the same on both nodes. The simplest configuration possible is:

```
resource test {
    on hasta {
        local /dev/ad6
        remote 172.16.0.2
    }
    on hastb {
        local /dev/ad6
        remote 172.16.0.1
    }
}
```

For more advanced configuration, refer to hast.conf(5).

It is also possible to use host names in the `remote` statements. In such a case, make sure that these hosts are resolvable and are defined in /etc/hosts or in the local DNS.

Now that the configuration exists on both nodes, the HAST pool can be created. Run these commands on both nodes to place the initial metadata onto the local disk and to start hastd(8):

```
# hastctl create test
# service hastd onestart
```

It is *not* possible to use GEOM providers with an existing file system or to convert an existing storage to a HAST-managed pool. This procedure needs to store some metadata on the provider and there will not be enough required space available on an existing provider.

A HAST node's `primary` or `secondary` role is selected by an administrator, or software like Heartbeat, using hastctl(8). On the primary node, `hasta`, issue this command:

```
# hastctl role primary test
```

Similarly, run this command on the secondary node, `hastb`:

```
# hastctl role secondary test
```

When the nodes are unable to communicate with each other, and both are configured as primary nodes, the condition is called `split-brain`. To troubleshoot this situation, follow the steps described in Recovering from the Split-brain Condition.

Verify the result by running hastctl(8) on each node:

```
# hastctl status test
```

The important text is the `status` line, which should say `complete` on each of the nodes. If it says `degraded`, something went wrong. At this point, the synchronization between the nodes has already started. The synchronization completes when `hastctl status` reports 0 bytes of `dirty` extents.

The next step is to create a filesystem on the /dev/hast/test GEOM provider and mount it. This must be done on the `primary` node, as /dev/hast/test appears only on the `primary` node. Creating the filesystem can take a few minutes, depending on the size of the hard drive:

```
# newfs -U /dev/hast/test
# mkdir /hast/test
```

```
# mount /dev/hast/test /hast/test
```

Once the HAST framework is configured properly, the final step is to make sure that HAST is started automatically during system boot. Add this line to /etc/rc.conf:

```
hastd_enable="YES"
```

39.16.4.1. Failover Configuration

The goal of this example is to build a robust storage system which is resistant to the failure of any given node. The scenario is that a `primary` node of the cluster fails. If this happens, the `secondary` node is there to take over seamlessly, check and mount the file system, and continue to work without missing a single bit of data.

To accomplish this task, another FreeBSD feature, CARP, provides for automatic failover on the IP layer. CARP (Common Address Redundancy Protocol) allows multiple hosts on the same network segment to share an IP address. Set up CARP on both nodes of the cluster according to the documentation available in Common Access Redundancy Protocol (CARP). After setup, each node will have its own carp0 interface with a shared IP address of *172.16.0.254*. The primary HAST node of the cluster must be the master CARP node.

The HAST pool created in the previous section is now ready to be exported to the other hosts on the network. This can be accomplished by exporting it through NFS or Samba, using the shared IP address *172.16.0.254*. The only problem which remains unresolved is an automatic failover should the primary node fail.

In the event of CARP interfaces going up or down, the FreeBSD operating system generates a devd(8) event, making it possible to watch for state changes on the CARP interfaces. A state change on the CARP interface is an indication that one of the nodes failed or came back online. These state change events make it possible to run a script which will automatically handle the HAST failover.

To be able to catch state changes on the CARP interfaces, add this configuration to /etc/devd.conf on each node:

```
notify 30 {
    match "system" "IFNET";
    match "subsystem" "carp0";
    match "type" "LINK_UP";
    action "/usr/local/sbin/carp-hast-switch master";
};

notify 30 {
    match "system" "IFNET";
    match "subsystem" "carp0";
    match "type" "LINK_DOWN";
    action "/usr/local/sbin/carp-hast-switch slave";
};
```

Restart devd(8) on both nodes to put the new configuration into effect:

```
# service devd restart
```

When the carp0 interface state changes by going up or down , the system generates a notification, allowing the devd(8) subsystem to run an arbitrary script, in this case /usr/local/sbin/carp-hast-switch. This script handles the automatic failover. For further clarification about the above devd(8) configuration, refer to devd.conf(5).

An example of such a script could be:

```
#!/bin/sh

# Original script by Freddie Cash <fjwcash@gmail.com>
# Modified by Michael W. Lucas <mwlucas@BlackHelicopters.org>
# and Viktor Petersson <vpetersson@wireload.net>

# The names of the HAST resources, as listed in /etc/hast.conf
resources="test"

# delay in mounting HAST resource after becoming master
# make your best guess
delay=3

# logging
log="local0.debug"
name="carp-hast"

# end of user configurable stuff

case "$1" in
    master)
        logger -p $log -t $name "Switching to primary provider for ${resources}."
        sleep ${delay}

        # Wait for any "hastd secondary" processes to stop
        for disk in ${resources}; do
            while $( pgrep -lf "hastd: ${disk} \(secondary\)" > /dev/null 2>&1 ); do
                sleep 1
            done

            # Switch role for each disk
            hastctl role primary ${disk}
            if [ $? -ne 0 ]; then
                logger -p $log -t $name "Unable to change role to primary for resource
${disk}."
                exit 1
            fi
        done
```

```
        # Wait for the /dev/hast/* devices to appear
        for disk in ${resources}; do
            for I in $( jot 60 ); do
                [ -c "/dev/hast/${disk}" ] && break
                sleep 0.5
            done

            if [ ! -c "/dev/hast/${disk}" ]; then
                logger -p $log -t $name "GEOM provider /dev/hast/${disk} did not
appear."
                exit 1
            fi
        done

        logger -p $log -t $name "Role for HAST resources ${resources} switched to
primary."

        logger -p $log -t $name "Mounting disks."
        for disk in ${resources}; do
            mkdir -p /hast/${disk}
            fsck -p -y -t ufs /dev/hast/${disk}
            mount /dev/hast/${disk} /hast/${disk}
        done

    ;;

    slave)
        logger -p $log -t $name "Switching to secondary provider for ${resources}."

        # Switch roles for the HAST resources
        for disk in ${resources}; do
            if ! mount | grep -q "^/dev/hast/${disk} on "
            then
            else
                umount -f /hast/${disk}
            fi
            sleep $delay
            hastctl role secondary ${disk} 2>&1
            if [ $? -ne 0 ]; then
                logger -p $log -t $name "Unable to switch role to secondary for
resource ${disk}."
                exit 1
            fi
            logger -p $log -t $name "Role switched to secondary for resource ${disk}."
        done
    ;;
esac
```

In a nutshell, the script takes these actions when a node becomes `master` / `primary`:

- Promotes the HAST pools to primary on a given node.
- Checks the file system under the HAST pool.
- Mounts the pools at an appropriate place.

When a node becomes `backup` / `secondary`:

- Unmounts the HAST pools.
- Degrades the HAST pools to secondary.

Keep in mind that this is just an example script which serves as a proof of concept. It does not handle all the possible scenarios and can be extended or altered in any way, for example, to start/stop required services.

For this example, a standard UFS file system was used. To reduce the time needed for recovery, a journal-enabled UFS or ZFS file system can be used instead.

More detailed information with additional examples can be found in the HAST Wiki page.

39.16.5. Troubleshooting

39.16.5.1. General Troubleshooting Tips

HAST should generally work without issues. However, as with any other software product, there may be times when it does not work as supposed. The sources of the problems may be different, but the rule of thumb is to ensure that the time is synchronized between all nodes of the cluster.

When troubleshooting HAST problems, the debugging level of hastd(8) should be increased by starting hastd(8) with `-d`. This argument may be specified multiple times to further increase the debugging level. A lot of useful information may be obtained this way. Consider also using `-F`, which starts hastd(8) in the foreground.

39.16.5.2. Recovering from the Split-brain Condition

`Split-brain` is when the nodes of the cluster are unable to communicate with each other, and both are configured as primary. This is a dangerous condition because it allows both nodes to make incompatible changes to the data. This problem must be corrected manually by the system administrator.

The administrator must decide which node has more important changes (or merge them manually) and let HAST perform full synchronization of the node which has the broken data. To do this, issue these commands on the node which needs to be resynchronized:

```
# hastctl role init <resource>
# hastctl create <resource>
# hastctl role secondary <resource>
```

Chapter 40. GEOM: Διαχείριση Συστοιχιών Δίσκων

40.1. Σύνοψη

Το κεφάλαιο αυτό καλύπτει τη χρήση των δίσκων κάτω από το πλαίσιο λειτουργιών GEOM στο FreeBSD. Περιλαμβάνει τα κυριότερα προγράμματα ελέγχου RAID των οποίων οι ρυθμίσεις βασίζονται στο πλαίσιο GEOM. Το κεφάλαιο αυτό δεν αναλύει σε βάθος τον τρόπο με τον οποίο το GEOM χειρίζεται ή ελέγχει λειτουργίες Εισόδου / Εξόδου (IO), το υποσύστημα που βρίσκεται κάτω από αυτό, ή τον κώδικα του. Οι πληροφορίες αυτές παρέχονται από τη σελίδα manual του geom(4) καθώς και από τις αναφορές που περιέχει σε άλλες σχετικές σελίδες. Επίσης το κεφάλαιο αυτό δεν αποτελεί καθοριστικό οδηγό για όλες τις ρυθμίσεις του RAID. Θα συζητηθούν μόνο οι καταστάσεις λειτουργίας του RAID που υποστηρίζονται από το GEOM.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Το είδος της υποστήριξης RAID που είναι διαθέσιμο μέσω του GEOM.
- Πως να χρησιμοποιήσετε τα βασικά βοηθητικά προγράμματα για την ρύθμιση, συντήρηση και διαχείριση των διαφόρων επιπέδων RAID.
- Πως να δημιουργήσετε mirror ή stripe, να κρυπτογραφήσετε, και να συνδέσετε δίσκους με το GEOM, μέσω μιας απομακρυσμένης σύνδεσης.
- Πως να αντιμετωπίσετε προβλήματα δίσκων που χρησιμοποιούν το πλαίσιο λειτουργιών GEOM.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε πως μεταχειρίζεται το FreeBSD τις συσκευές δίσκων (Αποθηκευτικά Μέσα).
- Να γνωρίζετε πως θα ρυθμίσετε και θα εγκαταστήσετε ένα νέο πυρήνα στο FreeBSD (Ρυθμίζοντας τον Πυρήνα του FreeBSD).

40.2. Εισαγωγή στο GEOM

Το GEOM επιτρέπει την πρόσβαση και τον έλεγχο σε κλάσεις - όπως την Κεντρική Εγγραφή Εκκίνησης (Master Boot Record), τα BSD labels, κ.α. - μέσω της χρήσης παροχέων, ή μέσω ειδικών αρχείων στον κατάλογο /dev. Το GEOM υποστηρίζει διάφορες διατάξεις RAID και παρέχει διάφανη πρόσβαση στο λειτουργικό σύστημα και τα βοηθητικά του προγράμματα.

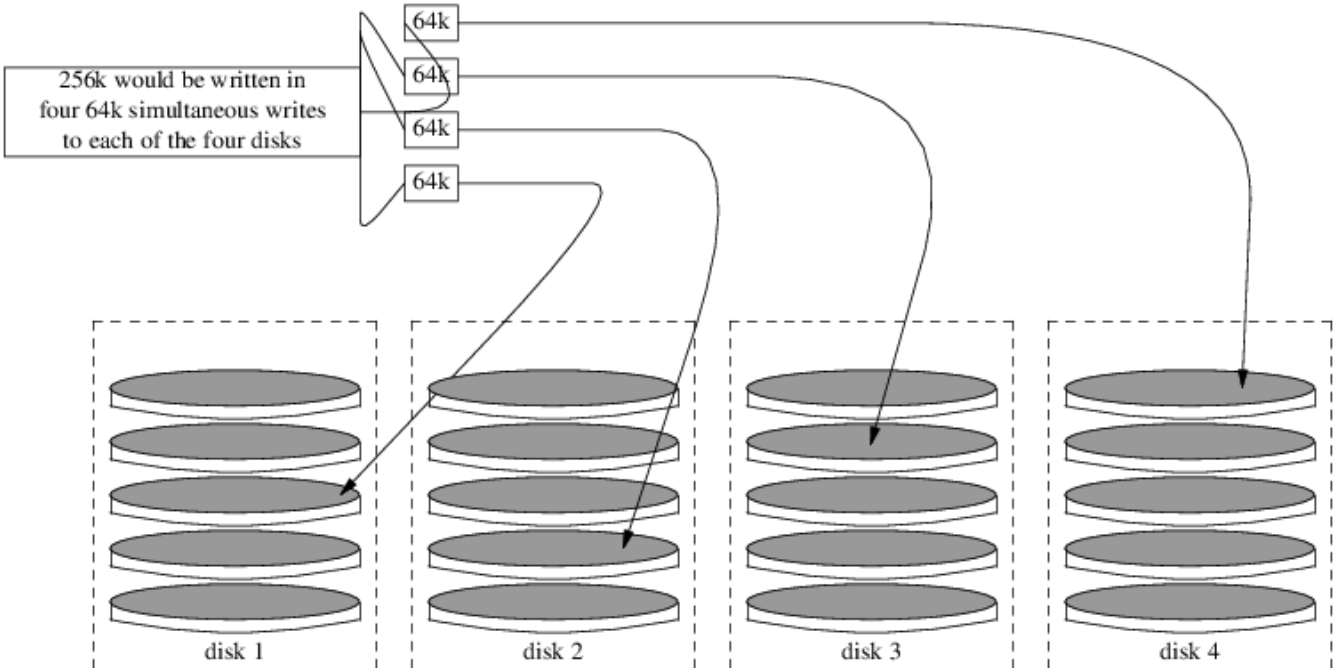
40.3. RAID0 - Striping

Το striping είναι μια μέθοδος που συνδυάζει διαφορετικούς φυσικούς δίσκους σε ένα μοναδικό λογικό τόμο. Σε πολλές περιπτώσεις, αυτό γίνεται με την βοήθεια εξειδικευμένου υλικού (ελεγκτών). Το υποσύστημα δίσκων GEOM παρέχει υποστήριξη μέσω λογισμικού για τη διάταξη RAID0, η οποία είναι γνωστή και ως striping.

Σε ένα σύστημα RAID0, τα δεδομένα χωρίζονται σε blocks τα οποία γράφονται τμηματικά σε όλους τους δίσκους που αποτελούν τη συστοιχία. Αντί να χρειάζεται να περιμένετε το σύστημα να γράψει

256k δεδομένων σε ένα δίσκο, ένα σύστημα RAID0 μπορεί να γράψει ταυτόχρονα 64k σε καθένα από τους τέσσερις δίσκους μιας συστοιχίας, προσφέροντας έτσι εξαιρετική απόδοση εισόδου/εξόδου (I/O). Η απόδοση αυτή μπορεί να αυξηθεί περισσότερο, με τη χρήση πολλαπλών ελεγκτών δίσκων.

Κάθε δίσκος σε ένα stripe RAID0 πρέπει να είναι του ίδιου μεγέθους, καθώς οι αιτήσεις I/O μοιράζονται όσο αφορά την ανάγνωση και εγγραφή, σε πολλούς παράλληλους δίσκους.



Procedure: Δημιουργία Stripe από μη-Διαμορφωμένους ATA Δίσκους

1. Φορτώστε το άρθρωμα geom_stripe.ko:

```
# kldload geom_stripe
```

2. Εξασφαλίστε ότι υπάρχει κατάλληλο σημείο προσάρτησης. Αν ο τόμος πρόκειται να γίνει κατάτμηση root, προσαρτήστε τον προσωρινά σε κάποιο άλλο σημείο προσάρτησης, όπως το /mnt:

```
# mkdir /mnt
```

3. Καθορίστε τα ονόματα των συσκευών για τους δίσκους που πρόκειται να γίνουν stripe, και δημιουργήστε τη νέα συσκευή stripe. Για παράδειγμα, για να δημιουργήσετε ένα stripe από δύο αχρησιμοποίητους και χωρίς κατατμήσεις δίσκους ATA, όπως π.χ. τους /dev/ad2 και /dev/ad3:

```
# gstripe label -v st0 /dev/ad2 /dev/ad3
Metadata value stored on /dev/ad2.
Metadata value stored on /dev/ad3.
Done.
```

4. Γράψτε ένα τυποποιημένο label (πίνακα κατατμήσεων) στο νέο τόμο, και εγκαταστήστε τον προεπιλεγμένο κώδικα εκκίνησης (bootstrap):

```
# bsdlabel -wB /dev/stripe/st0
```

5. Η διαδικασία αυτή θα δημιουργήσει τη συσκευή st0, καθώς και δύο ακόμα συσκευές στον κατάλογο /dev/stripe. Οι συσκευές αυτές θα ονομάζονται st0a και st0c. Στο σημείο αυτό, μπορείτε πλέον να δημιουργήσετε σύστημα αρχείων στη συσκευή st0a χρησιμοποιώντας το βοηθητικό πρόγραμμα `newfs`:

```
# newfs -U /dev/stripe/st0a
```

   Θα δείτε μια μεγάλη σειρά αριθμών να περνά γρήγορα από την οθόνη σας, και μετά από λίγα δευτερόλεπτα η διαδικασία θα έχει ολοκληρωθεί. Ο τόμος θα έχει δημιουργηθεί και θα είναι έτοιμος για προσάρτηση.

Για να προσαρτήσετε χειροκίνητα το stripe που δημιουργήσατε:

```
# mount /dev/stripe/st0a /mnt
```

Για να γίνεται αυτόματα η προσάρτηση αυτού του συστήματος αρχείων κατά την διαδικασία εκκίνησης, τοποθετήστε τις πληροφορίες του τόμου στο αρχείο /etc/fstab. Για το σκοπό αυτό, δημιουργούμε ένα μόνιμο σημείο προσάρτησης, το stripe:

```
# mkdir /stripe
# echo "/dev/stripe/st0a /stripe ufs rw 2 2" \
    >> /etc/fstab
```

Το άρθρωμα geom_stripe.ko θα πρέπει να φορτώνεται αυτόματα κατά την εκκίνηση του συστήματος. Εκτελέστε την παρακάτω εντολή, για να προσθέσετε την κατάλληλη ρύθμιση στο /boot/loader.conf:

```
# echo 'geom_stripe_load="YES"' >> /boot/loader.conf
```

40.4. RAID1 - Mirroring

Το mirroring (καθρεφτισμός) είναι μια τεχνολογία που χρησιμοποιείται από πολλές εταιρίες και οικιακούς χρήστες για να ασφαλίσουν τα δεδομένα τους χωρίς διακοπές. Σε μια διάταξη mirror, ο δίσκος Β είναι απλώς ένα πλήρες αντίγραφο του δίσκου Α. Ή μπορεί οι δίσκοι Γ+Δ να είναι αντίγραφα των δίσκων Α+Β. Άσχετα με την ακριβή διάταξη των δίσκων, το σημαντικό είναι ότι οι πληροφορίες ενός δίσκου ή μιας κατάτμησης αντιγράφονται σε άλλους. Οι πληροφορίες αυτές μπορεί αργότερα να αποκατασταθούν με εύκολο τρόπο, ή να αντιγραφούν χωρίς να προκληθεί

διακοπή στις υπηρεσίες του μηχανήματος ή στην πρόσβαση των δεδομένων. Μπορούν ακόμα και να μεταφερθούν και να φυλαχθούν σε άλλο, ασφαλές μέρος.

Για να ξεκινήσετε, βεβαιωθείτε ότι το σύστημα σας έχει δύο σκληρούς δίσκους ίδιου μεγέθους. Στα παραδείγματα μας θεωρούμε ότι οι δίσκοι είναι τύπου SCSI (απευθείας πρόσβασης, da(4)).

40.4.1. Mirroring στους Βασικούς Δίσκους

Υποθέτοντας ότι το FreeBSD έχει εγκατασταθεί στον πρώτο δίσκο da0, θα πρέπει να ρυθμίσετε το gmirror(8) να αποθηκεύσει εκεί τα βασικά δεδομένα του.

Πριν δημιουργήσετε το mirror, ενεργοποιήστε την δυνατότητα εμφάνισης περισσότερων λεπτομερειών (που μπορεί να σας βοηθήσουν σε περίπτωση προβλήματος) και επιτρέψτε την απευθείας πρόσβαση στη συσκευή δίσκου. Για το σκοπό αυτό θέστε τη μεταβλητή `kern.geom.debugflags` του sysctl(8) στην παρακάτω τιμή:

```
# sysctl kern.geom.debugflags=17
```

Μπορείτε τώρα να δημιουργήσετε το mirror. Ξεκινήστε τη διαδικασία αποθηκεύοντας τα μετα-δεδομένα (meta-data) στον βασικό δίσκο, δημιουργώντας ουσιαστικά τη συσκευή /dev/mirror/gm. Χρησιμοποιήστε την παρακάτω εντολή:

Η δημιουργία mirror στο δίσκο εκκίνησης μπορεί να έχει ως αποτέλεσμα την απώλεια δεδομένων, αν ο τελευταίος τομέας του δίσκου έχει ήδη χρησιμοποιηθεί. Η πιθανότητα αυτή είναι πολύ μικρότερη αν το mirror δημιουργηθεί αμέσως μετά από μια νέα εγκατάσταση του FreeBSD. Η παρακάτω διαδικασία είναι επίσης ασύμβατη με τις προεπιλεγμένες ρυθμίσεις εγκατάστασης του FreeBSD 9.*X* στις οποίες χρησιμοποιείται το σύστημα κατατμήσεων GPT. Το GEOM καταστρέφει τα μεταδεδομένα του GPT, και θα προκαλέσει απώλεια δεδομένων και πιθανή αδυναμία εκκίνησης του συστήματος.

```
# gmirror label -vb round-robin gm0 /dev/da0
```

Το σύστημα θα ανταποκριθεί με το παρακάτω μήνυμα:

```
Metadata value stored on /dev/da0.
Done.
```

Αρχικοποιήστε το GEOM. Η παρακάτω εντολή θα φορτώσει το άρθρωμα /boot/kernel/geom_mirror.ko στον πυρήνα:

```
# gmirror load
```

Με την επιτυχή εκτέλεση αυτής της εντολής, δημιουργείται η συσκευή gm0 μέσα

στον κατάλογο /dev/mirror.

Ενεργοποιήστε το φόρτωμα του αρθρώματος geom_mirror.ko κατά την εκκίνηση του συστήματος:

```
# echo 'geom_mirror_load="YES"' >> /boot/loader.conf
```

Επεξεργαστείτε το αρχείο /etc/fstab, αντικαθιστώντας τις αναφορές στις παλιές συσκευές da0 με τις αντίστοιχες καινούριες gm0 που αντιπροσωπεύουν το mirror.

Αν χρησιμοποιείτε το vi(1), μπορείτε να ακολουθήσετε τα παρακάτω βήματα για να ολοκληρώσετε εύκολα αυτή τη διαδικασία:

```
# vi /etc/fstab
```

Στο vi(1), κρατήστε αντίγραφο ασφαλείας του τρέχοντος αρχείου fstab πληκτρολογώντας `:w /etc/fstab.bak`. Έπειτα αντικαταστήστε όλες τις αναφορές στις παλιές συσκευές da0 με τις νέες gm0 γράφοντας `:%s/da/mirror\/gm/g`.

Το fstab που θα προκύψει, θα μοιάζει με το παρακάτω. Δεν έχει σημασία αν οι δίσκοι ήταν αρχικά SCSI ή ATA, η συσκευή RAID θα έχει πάντα το όνομα gm.

```
# Device                Mountpoint  FStype      Options   Dump     Pass#
/dev/mirror/gm0s1b      none        swap        sw        0        0
/dev/mirror/gm0s1a      /           ufs         rw        1        1
/dev/mirror/gm0s1d      /usr        ufs         rw        0        0
/dev/mirror/gm0s1f      /home       ufs         rw        2        2
#/dev/mirror/gm0s2d     /store      ufs         rw        2        2
/dev/mirror/gm0s1e      /var        ufs         rw        2        2
/dev/acd0               /cdrom      cd9660      ro,noauto 0        0
```

Επανεκκινήστε το σύστημα:

```
# shutdown -r now
```

Κατά την εκκίνηση του συστήματος, θα πρέπει πλέον να χρησιμοποιείται η συσκευή gm0 αντί για την da0. Μετά το τέλος της εκκίνησης, μπορείτε να ελέγξετε ότι όλα λειτουργούν σωστά, εξετάζοντας την έξοδο της εντολής `mount`:

```
# mount
Filesystem         1K-blocks    Used    Avail Capacity  Mounted on
/dev/mirror/gm0s1a   1012974  224604   707334    24%    /
devfs                      1       1        0   100%    /dev
/dev/mirror/gm0s1f  45970182   28596 42263972     0%    /home
/dev/mirror/gm0s1d   6090094 1348356  4254532    24%    /usr
/dev/mirror/gm0s1e   3045006 2241420   559986    80%    /var
```

```
devfs                   1      1        0   100%    /var/named/dev
```

Η έξοδος φαίνεται σωστή, όπως αναμενόταν. Τελικά, για να ξεκινήσει ο συγχρονισμός, εισάγετε και την συσκευή da1 στο mirror, χρησιμοποιώντας την ακόλουθη εντολή:

```
# gmirror insert gm0 /dev/da1
```

Κατά τη διάρκεια του συγχρονισμού του mirror, μπορείτε να δείτε την πρόοδο της διαδικασίας με την παρακάτω εντολή:

```
# gmirror status
```

Μετά το τέλος της δόμησης του mirror, και αφού έχουν συγχρονιστεί όλα τα δεδομένα, η έξοδος της παραπάνω εντολής θα μοιάζει με την ακόλουθη:

```
      Name    Status  Components
mirror/gm0  COMPLETE  da0
                      da1
```

Αν υπάρχουν προβλήματα, ή αν το mirror βρίσκεται ακόμα στη διαδικασία συγχρονισμού, το παράδειγμα θα δείχνει `DEGRADED` αντί για `COMPLETE`.

40.4.2. Αντιμετώπιση Προβλημάτων

40.4.2.1. Το σύστημα αρνείται να ξεκινήσει

Αν το σύστημα σας σταματάει σε μια προτροπή που μοιάζει με την παρακάτω:

```
ffs_mountroot: can't find rootvp
Root mount failed: 6
mountroot>
```

Επανεκκινήστε το σύστημα σας μέσω του διακόπτη τροφοδοσίας ή του πλήκτρου reset. Στο μενού εκκίνησης, επιλέξτε το (6). Με τον τρόπο αυτό θα βρεθείτε στην προτροπή του loader(8). Φορτώστε χειροκίνητα το άρθρωμα στον πυρήνα:

```
OK? load geom_mirror
OK? boot
```

Αν το παραπάνω λειτουργήσει, τότε για κάποιο λόγο το άρθρωμα δεν φορτώθηκε σωστά. Ελέγξτε αν είναι σωστή η σχετική καταχώριση στο αρχείο /boot/loader.conf. Αν το πρόβλημα παραμένει, προσθέστε τη γραμμή:

```
options GEOM_MIRROR
```

στο αρχείο ρυθμίσεων του πυρήνα σας, αναδημιουργήστε και επανεγκαταστήστε τον πυρήνα σας. Το πρόβλημα σας θα πρέπει να διορθωθεί.

40.4.3. Επαναφορά Μετά από Αποτυχία Δίσκου

Το εκπληκτικό με το mirroring είναι ότι όταν ένας σκληρός δίσκος χαλάσει, μπορείτε να τον αντικαταστήσετε χωρίς να χάσετε καθόλου δεδομένα.

Υποθέτοντας ότι χρησιμοποιούμε τις ρυθμίσεις RAID1 που δείξαμε προηγουμένως, ας θεωρήσουμε ότι χάλασε ο δίσκος da1 και πρέπει να αντικατασταθεί. Για να τον αντικαταστήσετε, βρείτε ποιος δίσκος είναι και απενεργοποιήστε το σύστημα. Στο σημείο αυτό, μπορείτε πλέον να ανταλλάξετε το δίσκο με ένα νέο και να ενεργοποιήσετε ξανά το σύστημα. Μετά την επανενεργοποίηση του συστήματος, μπορείτε να χρησιμοποιήσετε τις παρακάτω εντολές για να θέσετε σε λειτουργία το νέο δίσκο:

```
# gmirror forget gm0
```

```
# gmirror insert gm0 /dev/da1
```

Χρησιμοποιήστε την εντολή `gmirror status` για να παρακολουθείτε τη διαδικασία του συγχρονισμού. Είναι στα αλήθεια τόσο απλό.

40.5. RAID3 - Striping σε Επίπεδο Byte με Αφοσιωμένο Parity

Το RAID3 είναι μια μέθοδος που συνδυάζει αρκετούς διαφορετικούς σκληρούς δίσκους σε ένα τόμο με ένα δίσκο αφοσιωμένο στην ισοτιμία (parity). Σε ένα σύστημα RAID3, τα δεδομένα χωρίζονται σε ένα αριθμό από bytes που εγγράφονται σε όλους τους δίσκους της συστοιχίας εκτός από ένα που χρησιμοποιείται αποκλειστικά ως δίσκος ισοτιμίας. Αυτό σημαίνει ότι για να διαβάσουμε 1024KB από μια υλοποίηση του RAID3 θα πρέπει να προσπελάσουμε όλους τους δίσκους της συστοιχίας. Η απόδοση αυξάνεται με τη χρήση χωριστών ελεγκτών σκληρών δίσκων. Η συστοιχία RAID3 προσφέρει ανοχή σε βλάβη ενός δίσκου ενός παρέχει χωρητικότητα 1 - 1/n φορές τη χωρητικότητα όλων των δίσκων της συστοιχίας, όπου n είναι το πλήθος των δίσκων που την απαρτίζουν. Αυτού του είδους οι συστοιχίες είναι κατάλληλες για αποθήκευση μεγάλων αρχείων, για παράδειγμα αρχείων πολυμέσων.

Χρειάζονται τουλάχιστον 3 φυσικοί σκληροί δίσκοι για τη δημιουργία μια συστοιχίας RAID3. Κάθε δίσκος θα πρέπει να είναι το ίδιο μέγεθος καθώς οι αιτήσεις I/O (εισόδου/εξόδου) εναλλάσσονται ώστε να γίνεται εγγραφή και ανάγνωση σε πολλαπλούς δίσκους παράλληλα. Επίσης, εξαιτίας της φύσης του RAID3, ο αριθμός των δίσκων πρέπει να είναι 3, 5, 9, 17 κλπ. (2^n+1).

40.5.1. Δημιουργία Συστοιχίας RAID3

Στο FreeBSD, η υποστήριξη για RAID3 υλοποιείται μέσω της κλάσης graid3(8) του GEOM. Η δημιουργία μιας συστοιχίας RAID3 στο FreeBSD απαιτεί τα παρακάτω βήματα.

Αν και είναι θεωρητικά δυνατό να φτιάξετε μια εκκινήσιμη συστοιχία RAID3 στο FreeBSD, δεν συνίσταται καθώς πρόκειται για ασυνήθιστη λειτουργία.

1. Αρχικά, φορτώστε το geom_rai3.ko άρθρωμα του πυρήνα μέσω της ακόλουθης εντολής:

```
# graid3 load
```

   Εναλλακτικά, είναι δυνατόν να φορτώσετε το άρθρωμα χειροκίνητα:

```
# kldload geom_raid3.ko
```

2. Εξασφαλίστε ότι υπάρχει κατάλληλο σημείο προσάρτησης, ή δημιουργήστε ένα καινούριο:

```
# mkdir /multimedia
```

3. Προσδιορίστε τα ονόματα συσκευών των δίσκων που θα προστεθούν στη συστοιχία και δημιουργήστε τη νέα συσκευή RAID3. Στο παράδειγμα μας χρησιμοποιούμε τρεις οδηγούς ATA οι οποίοι δεν περιέχουν κατατμήσεις: ada1 και ada2 για τα δεδομένα και ada3 για το parity.

```
# graid3 label -v gr0 /dev/ada1 /dev/ada2 /dev/ada3
Metadata value stored on /dev/ada1
Metadata value stored on /dev/ada2
Metadata value stored on /dev/ada3
Done.
```

4. Δημιουργήστε κατατμήσεις στη νέα συσκευή gr0 και διαμορφώστε την με σύστημα αρχείων UFS:

```
# gpart create -s GPT /dev/raid3/gr0
# gpart add -t freebsd-ufs /dev/raid3/gr0
# newfs -j /dev/raid3/gr0p1
```

   Θα δείτε μεγάλο πλήθος αριθμών να περνάει από την οθόνη σας και μετά από λίγο η διαδικασία θα ολοκληρωθεί. Ο τόμος έχει πλέον δημιουργηθεί και είναι έτοιμος να προσαρτηθεί.

5. Το τελευταίο βήμα είναι η προσάρτηση του συστήματος αρχείων:

```
# mount /dev/raid3/gr0p1 /multimedia
```

Η συστοιχία RAID3 είναι τώρα έτοιμη προς χρήση.

Θα χρειαστεί να κάνετε επιπλέον ρυθμίσεις ώστε η συστοιχία να είναι άμεσα διαθέσιμη μετά από κάθε εκκίνηση του υπολογιστή σας.

1. Το άρθρωμα geom_raid3.ko θα πρέπει να φορτώνεται πριν την προσάρτηση της συστοιχίας. Για να φορτώνεται αυτόματα κατά την εκκίνηση του συστήματος, προσθέστε την παρακάτω γραμμή στο /boot/loader.conf:

   ```
   geom_raid3_load="YES"
   ```

2. Θα πρέπει να προσθέσετε τις παρακάτω πληροφορίες σχετικά με τον τόμο στο αρχείο /etc/fstab ώστε η προσάρτηση του συστήματος αρχείων της συστοιχίας να γίνεται αυτόματα κατά τη διαδικασία εκκίνησης του συστήματος:

   ```
   /dev/raid3/gr0p1    /multimedia    ufs    rw    2    2
   ```

40.6. Δικτυακές Συσκευές μέσω GEOM Gate

Το GEOM υποστηρίζει απομακρυσμένη χρήση συσκευών, όπως οι σκληροί δίσκοι, τα CD-ROM, τα αρχεία κ.λ.π. χρησιμοποιώντας τα βοηθητικά προγράμματα πύλης (gate). Η λειτουργία είναι παρόμοια με το NFS.

Για να ξεκινήσετε, πρέπει να δημιουργήσετε ένα αρχείο exports. Το αρχείο αυτό καθορίζει ποιος επιτρέπεται να αποκτήσει πρόσβαση στους κοινόχρηστους πόρους και τι επιπέδου θα είναι αυτή η πρόσβαση. Για παράδειγμα, για να διαμοιράσετε την τέταρτη κατάτμηση (slice) του πρώτου δίσκου SCSI, είναι αρκετό να δημιουργήσετε το παρακάτω αρχείο /etc/gg.exports:

```
192.168.1.0/24 RW /dev/da0s4d
```

Το παραπάνω θα επιτρέψει σε όλους τους υπολογιστές του ιδιωτικού σας δικτύου, να έχουν πρόσβαση μέσω δικτύου στο σύστημα αρχείων της κατάτμησης da0s4d.

Για να διαμοιράσετε αυτή τη συσκευή, βεβαιωθείτε ότι δεν είναι προσαρτημένη τη δεδομένη στιγμή, και ξεκινήστε το δαίμονα εξυπηρετητή ggated(8):

```
# ggated
```

Για να προσαρτήσετε την συσκευή στο μηχάνημα πελάτη, χρησιμοποιήστε τις ακόλουθες εντολές:

```
# ggatec create -o rw 192.168.1.1 /dev/da0s4d
ggate0
# mount /dev/ggate0 /mnt
```

Από εδώ και στο εξής, μπορείτε να έχετε πρόσβαση στη συσκευή μέσω του σημείου προσάρτησης /mnt.

Πρέπει να τονιστεί ότι η διαδικασία θα αποτύχει αν η συσκευή είναι τη δεδομένη στιγμή προσαρτημένη, είτε στον εξυπηρετητή, είτε σε οποιοδήποτε άλλο υπολογιστή στο δίκτυο.

Όταν δεν χρειάζεστε πλέον τη συσκευή, μπορείτε να την αποπροσαρτήσετε με ασφάλεια, χρησιμοποιώντας την εντολή umount(8), όπως γίνεται και με οποιαδήποτε άλλη συσκευή δίσκου.

40.7. Δημιουργώντας Ετικέτες (Labels) στις Συσκευές Δίσκων

Κατά τη διάρκεια της αρχικοποίησης, στην εκκίνηση του συστήματος, ο πυρήνας του FreeBSD θα δημιουργήσει τα απαραίτητα αρχεία για κάθε συσκευή που ανιχνεύει. Αυτή η μέθοδος ανίχνευσης συσκευών, μπορεί να δημιουργήσει προβλήματα. Για παράδειγμα, τι θα γίνει αν προσθέσουμε ένα νέο δίσκο USB; Είναι αρκετά πιθανό μια συσκευή μνήμης flash να πάρει το όνομα da0 και η αρχική da0 να μετακινηθεί στο da1. Αυτό θα προκαλέσει προβλήματα στην προσάρτηση των συστημάτων αρχείων, αν υπάρχουν οι αντίστοιχες καταχωρίσεις τους στο /etc/fstab, και μπορεί ακόμα και να παρεμποδίσει την κανονική εκκίνηση του συστήματος.

Μια λύση είναι να ρυθμίσετε τις συσκευές SCSI με τέτοιο τρόπο, ώστε η αρίθμηση τους να είναι συνεχόμενη. Έτσι, κάθε φορά που προσθέτετε μια νέα συσκευή στον ελεγκτή SCSI θα είστε σίγουρος ότι θα λάβει αριθμό που δεν έχει χρησιμοποιηθεί. Αλλά τι γίνεται με τις συσκευές USB που μπορεί να αντικαταστήσουν τον κύριο SCSI δίσκο; Αυτό μπορεί πράγματι να συμβεί, καθώς οι συσκευές USB ανιχνεύονται κατά βάση πριν από τον ελεγκτή SCSI. Μια λύση είναι να βάζετε τις συσκευές αυτές μόνο μετά την εκκίνηση του συστήματος. Μια άλλη μέθοδος είναι να χρησιμοποιείτε μόνο μια συσκευή τύπου ATA και να μην καταχωρείτε ποτέ τους δίσκους SCSI στο /etc/fstab.

Υπάρχει ωστόσο καλύτερη λύση. Χρησιμοποιώντας το βοηθητικό πρόγραμμα `glabel`, ένας διαχειριστής ή χρήστης, μπορεί να αποδώσει ετικέτες στις συσκευές δίσκων και να τις χρησιμοποιήσει στο /etc/fstab, αντί για τα συμβατικά ονόματα συσκευών. Επειδή η `glabel` αποθηκεύει την ετικέτα στον τελευταίο τομέα του κάθε παροχέα (συσκευής δίσκου), η ετικέτα διατηρείται και μετά από την επανεκκίνηση του συστήματος. Χρησιμοποιώντας αυτή την ετικέτα ως όνομα συσκευής, θα μπορείτε να προσαρτήσετε πάντα το σύστημα αρχείων, άσχετα με το πραγματικό όνομα συσκευής που έχει αποδοθεί στο δίσκο.

Δεν χρειάζεται φυσικά να τονίσουμε ότι αυτή η ετικέτα θα πρέπει να είναι μόνιμη. Το βοηθητικό πρόγραμμα `glabel` μπορεί να δημιουργήσει τόσο μόνιμες όσο και προσωρινές ετικέτες. Μόνο οι μόνιμες ετικέτες διατηρούνται ανέπαφες μετά από μια επανεκκίνηση. Δείτε τη σελίδα manual της glabel(8) για περισσότερες πληροφορίες σχετικά με τα είδη των ετικετών.

40.7.1. Είδη Ετικετών και Παραδείγματα

Υπάρχουν δύο τύποι ετικετών, η γενική ετικέτα και η ετικέτα συστήματος αρχείων. Οι ετικέτες μπορεί να είναι προσωρινές ή μόνιμες. Οι μόνιμες ετικέτες μπορούν να δημιουργηθούν με τις

εντολές tunefs(8) ή newfs(8). Στην περίπτωση αυτή, θα δημιουργηθούν σε ένα υποκατάλογο του /dev. Για παράδειγμα, οι ετικέτες συσκευών με σύστημα αρχείων UFS2, θα δημιουργηθούν στον κατάλογο /dev/ufs. Μόνιμες ετικέτες μπορούν επίσης να δημιουργηθούν με χρήση της εντολής `glabel label`. Οι ετικέτες αυτές δεν εξαρτώνται από το σύστημα αρχείων, και δημιουργούνται στον κατάλογο /dev/label.

Οι ετικέτες προσωρινού τύπου, χάνονται σε κάθε επανεκκίνηση του συστήματος. Οι ετικέτες αυτές δημιουργούνται στον κατάλογο /dev/label και είναι τέλειες για πειραματισμούς. Μπορείτε να δημιουργήσετε προσωρινές ετικέτες με την εντολή `glabel create`. Για περισσότερες πληροφορίες, διαβάστε τη σελίδα manual της glabel(8).

Για να δημιουργήσετε μια μόνιμη ετικέτα για ένα σύστημα αρχείων UFS2, χωρίς να καταστρέψετε τα δεδομένα που περιέχει, χρησιμοποιήστε την ακόλουθη εντολή:

```
# tunefs -L home /dev/da3
```

Αν το σύστημα αρχείων είναι γεμάτο, η παραπάνω εντολή μπορεί να προκαλέσει καταστροφή δεδομένων. Ωστόσο, αν το σύστημα αρχείων είναι γεμάτο, στόχος σας θα πρέπει να είναι να διαγράψετε τα αρχεία που δεν χρησιμοποιούνται, και όχι να προσθέτετε ετικέτες.

Θα πρέπει τώρα να υπάρχει μια ετικέτα στον κατάλογο /dev/ufs η οποία μπορεί να προστεθεί στο /etc/fstab:

```
/dev/ufs/home       /home           ufs     rw              2       2
```

Το σύστημα αρχείων δεν πρέπει να είναι προσαρτημένο καθώς εκτελείτε την εντολή `tunefs`.

Μπορείτε τώρα να προσαρτήσετε το σύστημα αρχείων με το συνήθη τρόπο:

```
# mount /home
```

Από εδώ και πέρα, και όσο το άρθρωμα geom_label.ko φορτώνεται στον πυρήνα μέσω του /boot/loader.conf ή εφόσον έχετε βάλει την επιλογή `GEOM_LABEL` στον πυρήνα σας, ακόμα και αν το όνομα της συσκευής αλλάξει, δεν θα έχει καμιά δυσμενή επίδραση στο σύστημα σας.

Μπορείτε επίσης να δημιουργήσετε συστήματα αρχείων με προεπιλεγμένη ετικέτα, χρησιμοποιώντας την επιλογή `-L` στην εντολή `newfs`. Δείτε την σελίδα manual του newfs(8) για περισσότερες πληροφορίες.

Μπορείτε να χρησιμοποιήσετε την παρακάτω εντολή για να καταστρέψετε μια ετικέτα:

```
# glabel destroy home
```

Το επόμενο παράδειγμα δείχνει πως μπορούν να δοθούν ετικέτες στις κατατμήσεις του δίσκου εκκίνησης.

Παράδειγμα 19. Δημιουργία Ετικετών στις Κατατμήσεις του Δίσκου Εκκίνησης

Δημιουργώντας μόνιμες ετικέτες στις κατατμήσεις του δίσκου εκκίνησης, το σύστημα σας θα συνεχίσει να εκκινεί κανονικά ακόμα και αν μεταφέρετε το δίσκο σε άλλο ελεγκτή ή ακόμα και σε διαφορετικό σύστημα. Στο παράδειγμα μας, θεωρούμε ότι χρησιμοποιείται ένας δίσκος ATA, ο οποίος αναγνωρίζεται από το σύστημα ως ad0. Θεωρούμε επίσης ότι χρησιμοποιείται η συνηθισμένη διάταξη κατατμήσεων του FreeBSD, που περιλαμβάνει τις κατατμήσεις /, /var, /usr και /tmp όπως επίσης και μια κατάτμηση swap.

Επανεκκινήστε το σύστημα, και όταν εμφανιστεί η προτροπή του loader(8), πιέστε το `4` για να πραγματοποιηθεί εκκίνηση σε κατάσταση ενός χρήστη. Έπειτα, δώστε τις ακόλουθες εντολές:

```
# glabel label rootfs /dev/ad0s1a
GEOM_LABEL: Label for provider /dev/ad0s1a is label/rootfs
# glabel label var /dev/ad0s1d
GEOM_LABEL: Label for provider /dev/ad0s1d is label/var
# glabel label usr /dev/ad0s1f
GEOM_LABEL: Label for provider /dev/ad0s1f is label/usr
# glabel label tmp /dev/ad0s1e
GEOM_LABEL: Label for provider /dev/ad0s1e is label/tmp
# glabel label swap /dev/ad0s1b
GEOM_LABEL: Label for provider /dev/ad0s1b is label/swap
# exit
```

Η εκκίνηση θα συνεχιστεί κανονικά και το σύστημα θα έλθει σε κατάσταση πολλαπλών χρηστών (multi-user). Μετά το τέλος της εκκίνησης, επεξεργαστείτε το αρχείο /etc/fstab και αλλάξτε τα συμβατικά ονόματα συσκευών με τις αντίστοιχες ετικέτες. Το τελικό αρχείο /etc/fstab θα μοιάζει με το παρακάτω:

```
# Device                Mountpoint      FStype  Options         Dump    Pass#
/dev/label/swap         none            swap    sw              0       0
/dev/label/rootfs       /               ufs     rw              1       1
/dev/label/tmp          /tmp            ufs     rw              2       2
/dev/label/usr          /usr            ufs     rw              2       2
/dev/label/var          /var            ufs     rw              2       2
```

Μπορείτε τώρα να επανεκκινήσετε το σύστημα. Αν όλα πήγαν καλά, η εκκίνηση θα είναι κανονική, και η εντολή `mount` θα δείξει:

```
# mount
/dev/label/rootfs on / (ufs, local)
devfs on /dev (devfs, local)
/dev/label/tmp on /tmp (ufs, local, soft-updates)
/dev/label/usr on /usr (ufs, local, soft-updates)
```

```
/dev/label/var on /var (ufs, local, soft-updates)
```

Ξεκινώντας από το FreeBSD 7.2, το glabel(8) υποστηρίζει ένα νέο είδος ετικέτας για συστήματα αρχείων UFS, που βασίζεται σε ένα μοναδιαίο αναγνωριστικό τους, το `ufsid`. Οι ετικέτες αυτές βρίσκονται στον κατάλογο /dev/ufsid, δημιουργούνται αυτόματα κατά την εκκίνηση του συστήματος και είναι δυνατόν να χρησιμοποιηθούν για την προσάρτηση κατατμήσεων μέσω του /etc/fstab. Μπορείτε να χρησιμοποιήσετε την εντολή `glabel status` για να λάβετε μια λίστα των συστημάτων αρχείων με τις αντίστοιχες `ufsid` ετικέτες τους:

```
% glabel status
                  Name  Status  Components
ufsid/486b6fc38d330916     N/A  ad4s1d
ufsid/486b6fc16926168e     N/A  ad4s1f
```

Στο παραπάνω παράδειγμα, το ad4s1d αντιπροσωπεύει το σύστημα αρχείων /var, ενώ το ad4s1f αντιπροσωπεύει το σύστημα αρχείων /usr. Χρησιμοποιώντας τις τιμές `ufsid` που φαίνονται, η προσάρτηση αυτών των κατατμήσεων μπορεί να γίνει με τις παρακάτω καταχωρίσεις στο /etc/fstab:

```
/dev/ufsid/486b6fc38d330916        /var        ufs        rw        2      2
/dev/ufsid/486b6fc16926168e        /usr        ufs        rw        2      2
```

Οποιαδήποτε κατάτμηση διαθέτει αναγνωριστικό `ufsid` μπορεί να προσαρτηθεί με τον ίδιο τρόπο, χωρίς να υπάρχει πλέον ανάγκη να δημιουργηθεί μόνιμη ετικέτα χειροκίνητα. Η προσάρτηση μέσω ετικέτας `ufsid`, παρέχει το πλεονέκτημα της ανεξαρτησίας από το όνομα συσκευής, το οποίο παρέχουν και οι μόνιμες ετικέτες.

40.8. UFS Journaling Μέσω GEOM

Στην έκδοση 7.0 του FreeBSD υλοποιείται για πρώτη φορά η νέα (και από πολλούς αναμενόμενη) δυνατότητα για χρήση ημερολογίου (journal) στο σύστημα αρχείων. Η υλοποίηση παρέχεται μέσω του υποσυστήματος GEOM και μπορεί να ρυθμιστεί εύκολα μέσω του βοηθητικού προγράμματος gjournal(8).

Τι είναι το journaling; Το journaling αποθηκεύει σε ένα αρχείο καταγραφής (log, ημερολόγιο, ή απλώς journal) τις συναλλαγές του συστήματος αρχείων. Παράδειγμα συναλλαγής είναι οι αλλαγές που απαιτούνται για μια πλήρη διαδικασία εγγραφής στο δίσκο. Έτσι, στο log αποθηκεύονται οι αλλαγές στα μετα-δεδομένα (meta-data) και στα ίδια τα αρχεία, πριν γίνει η τελική (κανονική) αποθήκευση τους στο δίσκο. Το αρχείο καταγραφής μπορεί αργότερα να ξαναχρησιμοποιηθεί ώστε η συναλλαγή να γίνει από την αρχή, εξασφαλίζοντας με αυτό τον τρόπο ότι το σύστημα αρχείων θα παραμείνει σε σταθερή κατάσταση.

Πρόκειται ουσιαστικά για μια ακόμα μέθοδο προφύλαξης από απώλεια δεδομένων και ασυνέπειες στο σύστημα αρχείων. Σε αντίθεση με τα Soft Updates τα οποία εντοπίζουν και υποχρεώνουν την άμεση εγγραφή των μετα-δεδομένων, και των στιγμιοτύπων (Snapshots) τα οποία είναι εικόνες του συστήματος αρχείων σε μια δεδομένη στιγμή, το log αποθηκεύεται σε χώρο που έχει εκχωρηθεί

ειδικά για αυτό το σκοπό, και σε μερικές περιπτώσεις μπορεί να αποθηκεύεται σε εντελώς διαφορετικό δίσκο.

Σε αντίθεση με υλοποιήσεις journaling σε άλλα συστήματα αρχείων, η μέθοδος `gjournal` βασίζεται σε blocks, και δεν υλοποιείται ως μέρος του συστήματος αρχείων, αλλά μόνο ως επέκταση του GEOM.

Για ενεργοποίηση της υποστήριξης `gjournal`, θα πρέπει να υπάρχει η παρακάτω επιλογή στον πυρήνα του FreeBSD. Η επιλογή αυτή υπάρχει από προεπιλογή στην έκδοση 7.0 και όλες τις νεότερες εκδόσεις του FreeBSD.

```
options UFS_GJOURNAL
```

Αν χρειάζεται να προσαρτώνται τόμοι με journaling κατά την εκκίνηση, θα πρέπει επίσης να φορτώνεται αυτόματα και το άρθρωμα πυρήνα geom_journal.ko. Για το σκοπό αυτό, προσθέστε την παρακάτω γραμμή στο αρχείο /boot/loader.conf:

```
geom_journal_load="YES"
```

Εναλλακτικά, η λειτουργία αυτή μπορεί να ενσωματωθεί σε ένα προσαρμοσμένο πυρήνα, με την προσθήκη της παρακάτω γραμμής στο αντίστοιχο αρχείο ρυθμίσεων:

```
options GEOM_JOURNAL
```

Η δημιουργία journal σε ένα ελεύθερο σύστημα αρχείων, μπορεί τώρα να γίνει με τα ακόλουθα βήματα, θεωρώντας ότι η συσκευή da4 είναι ένας νέος δίσκος SCSI:

```
# gjournal load
# gjournal label /dev/da4
```

Στο σημείο αυτό θα υπάρχει μια συσκευή /dev/da4 καθώς και μια συσκευή /dev/da4.journal. Στη συσκευή αυτή μπορείτε τώρα να δημιουργήσετε σύστημα αρχείων:

```
# newfs -O 2 -J /dev/da4.journal
```

Η παραπάνω εντολή θα δημιουργήσει ένα σύστημα αρχείων UFS2 στη συσκευή /dev/da4.journal, η οποία έχει ήδη υποστήριξη για journaling.

Μπορείτε να χρησιμοποιήσετε την εντολή `mount` για να προσαρτήσετε την συσκευή στο επιθυμητό σημείο προσάρτησης, όπως φαίνεται παρακάτω:

```
# mount /dev/da4.journal /mnt
```

Στην περίπτωση αρκετών slice, θα δημιουργηθεί ένα journal για κάθε επιμέρους

> slice. Για παράδειγμα, αν υπάρχουν τα slices ad4s1 και ad4s2 τότε το `gjournal` θα δημιουργήσει τις συσκευές ad4s1.journal και ad4s2.journal.

Για καλύτερη απόδοση, ίσως είναι επιθυμητή η τήρηση του journal σε διαφορετικό δίσκο. Για τις περιπτώσεις αυτές, ο παροχέας ημερολογίου (η συσκευή δίσκου που θα περιέχει το journal) πρέπει να δίνεται ως παράμετρος στην εντολή, αμέσως μετά τη συσκευή δίσκου στην οποία θα ενεργοποιηθεί το journaling. Μπορείτε επίσης να ενεργοποιήσετε το journaling σε υπάρχοντα συστήματα αρχείων χρησιμοποιώντας την εντολή `tunefs`. Ωστόσο, θα πρέπει να κρατήσετε αντίγραφο ασφαλείας των αρχείων σας, πριν επιχειρήσετε να κάνετε αλλαγές σε ένα υπάρχον σύστημα αρχείων. Στις περισσότερες περιπτώσεις, η `tunefs` θα αποτύχει αν δεν μπορέσει να δημιουργήσει το journal, αλλά αυτό δεν σας προστατεύει από απώλεια δεδομένων που μπορεί να προέλθει από κακή χρήση της `tunefs`.

Είναι επίσης δυνατόν να χρησιμοποιηθεί journaling στον δίσκο εκκίνησης ενός συστήματος FreeBSD. Διαβάστε το άρθρο Υλοποίηση του UFS Journaling σε ένα Desktop Υπολογιστή για λεπτομερείς οδηγίες.

Chapter 41. Υποστήριξη Συστημάτων Αρχείων

41.1. Σύνοψη

Τα συστήματα αρχείων αποτελούν αναπόσπαστο τμήμα κάθε λειτουργικού συστήματος. Επιτρέπουν στους χρήστες να δημιουργούν και να αποθηκεύουν αρχεία, παρέχουν πρόσβαση σε δεδομένα, και φυσικά αξιοποιούν τους σκληρούς δίσκους. Διαφορετικά λειτουργικά συστήματα χρησιμοποιούν συνήθως διαφορετικά εγγενή συστήματα αρχείων. Το σύστημα αρχείων του FreeBSD είναι το Fast File System ή FFS, το οποίο προήλθε από το αρχικό σύστημα αρχείων του Unix™, γνωστό επίσης και ως UFS. Αυτό είναι και το εγγενές σύστημα αρχείων του FreeBSD, το οποίο χρησιμοποιείται στους σκληρούς δίσκους και προσφέρει πρόσβαση στα δεδομένα.

Το FreeBSD προσφέρει επίσης πληθώρα διαφορετικών συστημάτων αρχείων, ώστε να παρέχει τοπική πρόσβαση σε δεδομένα που έχουν δημιουργηθεί από άλλα λειτουργικά συστήματα, π.χ. δεδομένα που βρίσκονται σε τοπικά USB αποθηκευτικά μέσα, οδηγούς flash, και σκληρούς δίσκους. Υπάρχει επίσης υποστήριξη για άλλα, μη-εγγενή συστήματα αρχείων, όπως το Extended File System (EXT) του Linux® καθώς και το σύστημα Z File System (ZFS) της Sun™.

Το FreeBSD παρέχει διαφορετικό επίπεδο υποστήριξης για κάθε σύστημα αρχείων. Για ορισμένα θα χρειαστεί να φορτωθεί κάποιο άρθρωμα στον πυρήνα, ενώ για άλλα θα πρέπει να εγκατασταθούν κάποια εργαλεία. Το κεφάλαιο αυτό έχει σχεδιαστεί να βοηθήσει τους χρήστες του FreeBSD να αποκτήσουν πρόσβαση σε άλλα συστήματα αρχείων στο σύστημα τους, ξεκινώντας από το Z File System της Sun™.

Αφού διαβάσετε αυτό το κεφάλαιο, θα γνωρίζετε:

- Τη διαφορά μεταξύ των εγγενών και των υποστηριζόμενων συστημάτων αρχείων.
- Ποια συστήματα αρχείων υποστηρίζονται από το FreeBSD.
- Πως να ενεργοποιήσετε, να ρυθμίσετε, να αποκτήσετε πρόσβαση και να χρησιμοποιήσετε μη-εγγενή συστήματα αρχείων.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε βασικές έννοιες του UNIX® και του FreeBSD (Βασικές Έννοιες στο UNIX®).
- Να είστε εξοικειωμένος με τις βασικές διαδικασίες ρύθμισης και εγκατάστασης προσαρμοσμένου πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να αισθάνεστε άνετα με την εγκατάσταση εφαρμογών τρίτου κατασκευαστή στο FreeBSD (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).
- Να είστε εξοικειωμένος με τους δίσκους, τα μέσα αποθήκευσης, και τα αντίστοιχα ονόματα συσκευών στο FreeBSD (Αποθηκευτικά Μέσα).

41.2. Το Σύστημα Αρχείων Z (ZFS)

Το σύστημα αρχείων Z, αναπτύχθηκε από την Sun™, και είναι μια νέα τεχνολογία που σχεδιάστηκε

για να παρέχει αποθήκευση μέσω της μεθόδου pool. Αυτό σημαίνει ότι όλος ο ελεύθερος χώρος διατίθεται ως απόθεμα, και διανέμεται δυναμικά σε κάθε σύστημα αρχείων ανάλογα με τις ανάγκες αποθήκευσης δεδομένων. Έχει επίσης σχεδιαστεί για τη μέγιστη ακεραιότητα δεδομένων και υποστηρίζει στιγμιότυπα (snapshots) δεδομένων, πολλαπλά αντίγραφα και αθροίσματα ελέγχου δεδομένων (checksums). Έχει ακόμα προστεθεί ένα νέο μοντέλο για τη διατήρηση αντιγράφων των δεδομένων, γνωστό ως RAID-Z. Το μοντέλο RAID-Z είναι παρόμοιο με το RAID5 αλλά είναι σχεδιασμένο να παρέχει προστασία των δεδομένων κατά την εγγραφή τους.

41.2.1. Βελτιστοποίηση του ZFS

Το υποσύστημα ZFS χρησιμοποιεί αρκετούς πόρους του συστήματος. Βελτιστοποιώντας τις ρυθμίσεις του συστήματος σας, θα επιτύχετε τη μέγιστη απόδοση στην καθημερινή χρήση. Καθώς το ZFS είναι ακόμα σε πειραματικό στάδιο στο FreeBSD, αυτό ίσως αλλάξει μελλοντικά. Ωστόσο, για την ώρα, συνίσταται να ακολουθήσετε τα παρακάτω βήματα:

41.2.1.1. Μνήμη

Το συνολικό μέγεθος μνήμης του συστήματος πρέπει να είναι τουλάχιστον ένα gigabyte, ενώ το συνιστώμενο μέγεθος είναι δύο gigabytes ή και περισσότερο. Σε όλα τα παραδείγματα που φαίνονται εδώ, το σύστημα έχει ένα gigabyte μνήμης και έχουμε επίσης βελτιστοποιήσει τις ρυθμίσεις του.

Ορισμένοι χρήστες φαίνεται να τα καταφέρνουν και με λιγότερο από ένα gigabyte μνήμης, αλλά με τέτοιους περιορισμούς φυσικής μνήμης, είναι αρκετά πιθανό να δημιουργηθεί panic κάτω από βαρύ φορτίο εργασίας, εξαιτίας εξάντλησης της.

41.2.1.2. Ρύθμιση του Πυρήνα

Συνίσταται να αφαιρέσετε τα προγράμματα οδήγησης και τις επιλογές που δεν χρησιμοποιείτε από το αρχείο ρυθμίσεων του πυρήνα. Καθώς οι περισσότεροι οδηγοί συσκευών διατίθενται επίσης και σε μορφή αρθρωμάτων, μπορείτε να τους φορτώσετε χρησιμοποιώντας το αρχείο /boot/loader.conf.

Οι χρήστες της αρχιτεκτονικής i386™ θα πρέπει να προσθέσουν την παρακάτω επιλογή στο αρχείο ρυθμίσεων του πυρήνα τους, να τον επαναμεταγλωττίσουν και να επανεκκινήσουν το σύστημα τους:

```
options     KVA_PAGES=512
```

Η επιλογή αυτή θα διευρύνει την περιοχή διευθύνσεων του πυρήνα, επιτρέποντας έτσι την αύξηση τιμής της ρυθμιστικής μεταβλητής `vm.kvm_size` πέρα από το τρέχον όριο του 1 GB (2 GB για πυρήνες PAE). Για να βρείτε την καταλληλότερη τιμή για αυτή την επιλογή, διαιρέστε το επιθυμητό μέγεθος της περιοχής διευθύνσεων με το τέσσερα (4). Στην περίπτωση αυτή, έχουμε `512` για μέγεθος 2 GB.

41.2.1.3. Ρυθμίσεις στις Μεταβλητές του Loader

Θα πρέπει να αυξηθεί η περιοχή διευθύνσεων kmem σε όλες τις αρχιτεκτονικές του FreeBSD. Στο δοκιμαστικό μας σύστημα, με ένα gigabyte φυσικής μνήμης, είχαμε επιτυχημένο αποτέλεσμα χρησιμοποιώντας τις ακόλουθες επιλογές στο αρχείο /boot/loader.conf και επανεκκινώντας το

σύστημα μας:

```
vm.kmem_size="330M"
vm.kmem_size_max="330M"
vfs.zfs.arc_max="40M"
vfs.zfs.vdev.cache.size="5M"
```

Για αναλυτικότερες ρυθμίσεις σχετικά με την βελτιστοποίηση του ZFS, δείτε το http://wiki.freebsd.org/ZFSTuningGuide.

41.2.2. Χρησιμοποιώντας το ZFS

Υπάρχει ένας μηχανισμός εκκίνησης που επιτρέπει στο FreeBSD να προσαρτήσει ZFS pools κατά τη διάρκεια της εκκίνησης του συστήματος. Για να τον ρυθμίσετε, εκτελέστε τις ακόλουθες εντολές:

```
# echo 'zfs_enable="YES"' >> /etc/rc.conf
# /etc/rc.d/zfs start
```

Το υπόλοιπο αυτού του κειμένου υποθέτει ότι έχετε διαθέσιμους τρεις SCSI δίσκους, και ότι τα ονόματα συσκευών τους είναι da0, da1 και da2. Όσοι διαθέτουν δίσκους IDE θα πρέπει να χρησιμοποιήσουν συσκευές του τύπου ad αντί για τις αντίστοιχες SCSI.

41.2.2.1. Pool με Ένα Μόνο Δίσκο

Για την δημιουργία ενός ZFS pool με ένα μόνο δίσκο (χωρίς δυνατότητα ανοχής σφαλμάτων), χρησιμοποιήστε την εντολή `zpool`:

```
# zpool create example /dev/da0
```

Για να δείτε το νέο pool, εξετάστε την έξοδο της εντολής `df`:

```
# df
Filesystem  1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a   2026030  235230  1628718    13%    /
devfs               1       1        0   100%    /dev
/dev/ad0s1d  54098308 1032846 48737598     2%    /usr
example      17547136       0 17547136     0%    /example
```

Η έξοδος αυτή δείχνει καθαρά ότι το `example` pool όχι μόνο έχει δημιουργηθεί, αλλά έχει επίσης *προσαρτηθεί* κιόλας. Είναι επίσης διαθέσιμο ως κανονικό σύστημα αρχείων, μπορείτε να δημιουργήσετε αρχεία σε αυτό, και άλλοι χρήστες μπορούν επίσης να το δουν, όπως φαίνεται στο παρακάτω παράδειγμα:

```
# cd /example
# ls
```

```
# touch testfile
# ls -al
total 4
drwxr-xr-x   2 root  wheel    3 Aug 29 23:15 .
drwxr-xr-x  21 root  wheel  512 Aug 29 23:12 ..
-rw-r--r--   1 root  wheel    0 Aug 29 23:15 testfile
```

Δυστυχώς αυτό το pool δεν χρησιμοποιεί κάποιο από τα πλεονεκτήματα του ZFS. Δημιουργήστε ένα σύστημα αρχείων σε αυτό το pool και ενεργοποιήστε σε αυτό τη συμπίεση:

```
# zfs create example/compressed
# zfs set compression=gzip example/compressed
```

Το σύστημα αρχείων `example/compressed` είναι πλέον ένα συμπιεσμένο ZFS σύστημα. Δοκιμάστε να αντιγράψετε μερικά μεγάλα αρχεία σε αυτό, απευθείας στον κατάλογο /example/compressed.

Μπορείτε τώρα να απενεργοποιήσετε τη συμπίεση γράφοντας:

```
# zfs set compression=off example/compressed
```

Για να αποπροσαρτήσετε το σύστημα αρχείων, εκτελέστε την ακόλουθη εντολή και επαληθεύστε το αποτέλεσμα μέσω του βοηθητικού προγράμματος `df`:

```
# zfs umount example/compressed
# df
Filesystem  1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a   2026030  235232  1628716    13%    /
devfs               1       1        0   100%    /dev
/dev/ad0s1d  54098308 1032864 48737580     2%    /usr
example      17547008       0 17547008     0%    /example
```

Προσαρτήστε ξανά το σύστημα αρχείων, ώστε να είναι και πάλι προσβάσιμο, και επαληθεύστε το χρησιμοποιώντας όπως και πριν, την εντολή `df`:

```
# zfs mount example/compressed
# df
Filesystem         1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a          2026030  235234  1628714    13%    /
devfs                      1       1        0   100%    /dev
/dev/ad0s1d         54098308 1032864 48737580     2%    /usr
example             17547008       0 17547008     0%    /example
example/compressed  17547008       0 17547008     0%    /example/compressed
```

Μπορείτε επίσης να δείτε το pool και το σύστημα αρχείων εξετάζοντας την έξοδο της εντολής `mount`:

```
# mount
/dev/ad0s1a on / (ufs, local)
devfs on /dev (devfs, local)
/dev/ad0s1d on /usr (ufs, local, soft-updates)
example on /example (zfs, local)
example/data on /example/data (zfs, local)
example/compressed on /example/compressed (zfs, local)
```

Όπως παρατηρούμε, το σύστημα αρχείων ZFS μπορεί να χρησιμοποιηθεί ως κοινό σύστημα αρχείων μετά τη δημιουργία του. Ωστόσο, διαθέτει πολλές ακόμα λειτουργίες. Στο παρακάτω παράδειγμα δημιουργούμε ένα νέο σύστημα αρχείων, το `data`. θα αποθηκεύσουμε σημαντικά δεδομένα σε αυτό, και έτσι το ρυθμίζουμε ώστε να κρατάει δύο αντίγραφα από κάθε μπλοκ δεδομένων:

```
# zfs create example/data
# zfs set copies=2 example/data
```

Μπορούμε τώρα να δούμε τα δεδομένα και την κατανάλωση χώρου δίνοντας ξανά την εντολή `df`:

```
# df
Filesystem         1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a          2026030  235234  1628714    13%    /
devfs                      1       1        0   100%    /dev
/dev/ad0s1d         54098308 1032864 48737580     2%    /usr
example             17547008       0 17547008     0%    /example
example/compressed  17547008       0 17547008     0%    /example/compressed
example/data        17547008       0 17547008     0%    /example/data
```

Παρατηρήστε ότι κάθε σύστημα αρχείων στο pool δείχνει το ίδιο μέγεθος διαθέσιμου χώρου. Αυτός είναι και ο λόγος που χρησιμοποιούμε την εντολή `df` σε όλα τα παραδείγματα, για να δείξουμε ότι τα συστήματα αρχείων χρησιμοποιούν μόνο το χώρο που χρειάζονται και ότι όλα μοιράζονται τον ίδιο χώρο (το κοινόχρηστο απόθεμα - pool). Στο σύστημα αρχείων ZFS έννοιες όπως οι τόμοι (volumes) και οι κατατμήσεις (partitions) δεν έχουν νόημα. Αντίθετα, πολλά συστήματα αρχείων μοιράζονται τον ίδιο χώρο, το pool. Μπορείτε να καταργήσετε το σύστημα αρχείων και κατόπιν το ίδιο το pool όταν δεν τα χρειάζεστε πλέον:

```
# zfs destroy example/compressed
# zfs destroy example/data
# zpool destroy example
```

Οι σκληροί δίσκοι με τον καιρό χαλάνε, είναι αναπόφευκτο. Όταν ένας δίσκος χαλάσει, τα δεδομένα του χάνονται. Μια μέθοδος για να αποφύγουμε την απώλεια δεδομένων εξαιτίας ενός χαλασμένου δίσκου είναι να δημιουργήσουμε μια συστοιχία RAID. Τα pools του ZFS έχουν σχεδιασθεί ώστε να υποστηρίζουν αυτό το χαρακτηριστικό. Η λειτουργία αυτή αναλύεται στην επόμενη ενότητα.

41.2.2.2. ZFS RAID-Z

Όπως αναφέραμε προηγουμένως, η ενότητα αυτή προϋποθέτει ότι χρησιμοποιούμε τρεις συσκευές SCSI με ονόματα συσκευών da0, da1 και da2. Για να δημιουργήσουμε ένα pool τύπου RAID-Z, εκτελούμε την ακόλουθη εντολή:

```
# zpool create storage raidz da0 da1 da2
```

Η Sun™ συνιστά να χρησιμοποιούνται από τρεις ως εννιά συσκευές σε συστοιχίες τύπου RAID-Z. Αν χρειάζεται να δημιουργήσετε ένα pool με περισσότερους από δέκα δίσκους, είναι προτιμότερο να το χωρίσετε σε ομάδες από μικρότερα RAID-Z pools. Αν διαθέτετε μόνο δύο δίσκους αλλά χρειάζεστε την δυνατότητα ανοχής σφαλμάτων, ίσως είναι καλύτερο να χρησιμοποιήσετε ένα ZFS mirror. Δείτε τη σελίδα manual του zpool(8) για περισσότερες λεπτομέρειες.

Θα δημιουργηθεί το `storage` zpool. Μπορείτε να επαληθεύσετε το αποτέλεσμα χρησιμοποιώντας, όπως και προηγουμένως, τις εντολές mount(8) και df(1). Θα μπορούσαμε να χρησιμοποιήσουμε περισσότερους δίσκους, προσθέτοντας τα ονόματα συσκευών τους στο τέλος της παραπάνω λίστας. Δημιουργήστε ένα νέο σύστημα αρχείων στο pool, το οποίο θα ονομάζεται `home` και όπου θα αποθηκεύονται τελικά τα αρχεία των χρηστών:

```
# zfs create storage/home
```

Μπορούμε τώρα να ενεργοποιήσουμε την συμπίεση και να κρατάμε επιπλέον αντίγραφα των καταλόγων και των δεδομένων των χρηστών. Όπως και προηγουμένως, μπορούμε να το επιτύχουμε χρησιμοποιώντας τις παρακάτω εντολές:

```
# zfs set copies=2 storage/home
# zfs set compression=gzip storage/home
```

Για να γίνει αυτός ο νέος κατάλογος των χρηστών, αντιγράψτε τα δεδομένα τους σε αυτόν και δημιουργήστε τους κατάλληλους συμβολικούς δεσμούς:

```
# cp -rp /home/* /storage/home
# rm -rf /home /usr/home
# ln -s /storage/home /home
# ln -s /storage/home /usr/home
```

Τα δεδομένα των χρηστών θα αποθηκεύονται τώρα στο νέο σύστημα αρχείων /storage/home. Για να το επαληθεύσετε, δημιουργήστε ένα νέο χρήστη και εισέλθετε στο σύστημα με το νέο λογαριασμό.

Δοκιμάστε να δημιουργήσετε ένα στιγμιότυπο (snapshot) στο οποίο θα μπορείτε να επανέλθετε αργότερα:

```
# zfs snapshot storage/home@08-30-08
```

Σημειώστε ότι η επιλογή δημιουργίας στιγμιότυπου λειτουργεί μόνο σε πραγματικό σύστημα αρχείων, και όχι σε κάποιο μεμονωμένο κατάλογο ή αρχείο. Ο χαρακτήρας `@` χρησιμοποιείται ως διαχωριστικό μεταξύ του συστήματος αρχείων και του ονόματος τόμου. Αν καταστραφεί ο κατάλογος δεδομένων κάποιου χρήστη αποκαταστήστε τον με την εντολή:

```
# zfs rollback storage/home@08-30-08
```

Για να δείτε μια λίστα των διαθέσιμων στιγμιότυπων, εκτελέστε την εντολή `ls` στον κατάλογο .zfs/snapshot του συστήματος αρχείων. Για παράδειγμα, για να δείτε το στιγμιότυπο που δημιουργήσαμε προηγουμένως, εκτελέστε την παρακάτω εντολή:

```
# ls /storage/home/.zfs/snapshot
```

Είναι δυνατόν να γράψετε κάποιο script που να δημιουργεί μηνιαία στιγμιότυπα των δεδομένων των χρηστών. Ωστόσο, με την πάροδο του χρόνου, τα στιγμιότυπα θα καταναλώσουν μεγάλο ποσοστό του χώρου στο δίσκο. Μπορείτε να διαγράψετε το προηγούμενο στιγμιότυπο χρησιμοποιώντας την παρακάτω εντολή:

```
# zfs destroy storage/home@08-30-08
```

Δεν υπάρχει λόγος, μετά από όλες αυτές τις δοκιμές, να κρατήσουμε το /storage/home στην παρούσα κατάσταση του. Μετατρέψτε το στο πραγματικό σύστημα αρχείων /home:

```
# zfs set mountpoint=/home storage/home
```

Χρησιμοποιώντας τις εντολές `df` και `mount` θα δούμε ότι το σύστημα χειρίζεται πλέον αυτό το σύστημα αρχείων ως το πραγματικό /home:

```
# mount
/dev/ad0s1a on / (ufs, local)
devfs on /dev (devfs, local)
/dev/ad0s1d on /usr (ufs, local, soft-updates)
storage on /storage (zfs, local)
storage/home on /home (zfs, local)
# df
Filesystem   1K-blocks    Used    Avail Capacity  Mounted on
/dev/ad0s1a    2026030  235240  1628708    13%    /
devfs                1       1        0   100%    /dev
/dev/ad0s1d   54098308 1032826 48737618     2%    /usr
storage       26320512       0 26320512     0%    /storage
storage/home  26320512       0 26320512     0%    /home
```

Εδώ ολοκληρώνεται η ρύθμιση του RAID-Z. Για να δέχεστε αναφορές κατάστασης σχετικά με τα συστήματα αρχείων κατά τη νυκτερινή εκτέλεση του periodic(8), δώστε την παρακάτω εντολή:

```
# echo 'daily_status_zfs_enable="YES"' >> /etc/periodic.conf
```

41.2.2.3. Ανάκτηση του RAID-Z

Κάθε λογισμικό RAID έχει μια μέθοδο για επίβλεψη της κατάστασής του, και το ZFS δεν αποτελεί εξαίρεση. Μπορείτε να δείτε την κατάσταση των συσκευών του RAID-Z χρησιμοποιώντας την ακόλουθη εντολή:

```
# zpool status -x
```

Αν όλα τα pools είναι σε υγιή κατάσταση, θα πάρετε το ακόλουθο μήνυμα:

```
all pools are healthy
```

Αν υπάρχει κάποιο πρόβλημα, π.χ. κάποιος δίσκος έχει βγει εκτός λειτουργίας, θα δείτε την περιγραφή της κατάστασης σε ένα μήνυμα όπως το παρακάτω:

```
  pool: storage
 state: DEGRADED
status: One or more devices has been taken offline by the administrator.
    Sufficient replicas exist for the pool to continue functioning in a
    degraded state.
action: Online the device using 'zpool online' or replace the device with
    'zpool replace'.
 scrub: none requested
config:

    NAME        STATE     READ WRITE CKSUM
    storage     DEGRADED     0     0     0
      raidz1    DEGRADED     0     0     0
        da0     ONLINE       0     0     0
        da1     OFFLINE      0     0     0
        da2     ONLINE       0     0     0

errors: No known data errors
```

Το παραπάνω δείχνει ότι η συσκευή τέθηκε εκτός λειτουργίας από τον διαχειριστή. Αυτό είναι αλήθεια για το συγκεκριμένο παράδειγμα. Για να τεθεί ο δίσκος εκτός, χρησιμοποιήθηκε η παρακάτω εντολή:

```
# zpool offline storage da1
```

Μπορούμε τώρα να αντικαταστήσουμε το δίσκο da1 μετά την απενεργοποίηση του συστήματος. Όταν το σύστημα επανέλθει σε λειτουργία, μπορούμε να χρησιμοποιήσουμε την ακόλουθη εντολή για να ενημερώσουμε το σύστημα για την αντικατάσταση του δίσκου:

```
# zpool replace storage da1
```

Από εδώ, μπορούμε να ελέγξουμε ξανά την κατάσταση, αυτή τη φορά χωρίς την επιλογή `-x`:

```
# zpool status storage
 pool: storage
 state: ONLINE
 scrub: resilver completed with 0 errors on Sat Aug 30 19:44:11 2008
config:

    NAME        STATE     READ WRITE CKSUM
    storage     ONLINE       0     0     0
      raidz1    ONLINE       0     0     0
        da0     ONLINE       0     0     0
        da1     ONLINE       0     0     0
        da2     ONLINE       0     0     0

errors: No known data errors
```

Όπως φαίνεται στο παράδειγμα, τα πάντα φαίνεται να λειτουργούν φυσιολογικά.

41.2.2.4. Επαλήθευση Δεδομένων

Όπως αναφέραμε προηγουμένως, το ZFS χρησιμοποιεί `checksums` (αθροίσματα ελέγχου) για να επαληθεύσει την ακεραιότητα των αποθηκευμένων δεδομένων. Τα αθροίσματα ελέγχου ενεργοποιούνται αυτόματα κατά την δημιουργία των συστημάτων αρχείων, και μπορούν να απενεργοποιηθούν μέσω της επόμενης εντολής:

```
# zfs set checksum=off storage/home
```

Αυτό δεν είναι γενικά καλή ιδέα, καθώς τα checksums καταλαμβάνουν ελάχιστο αποθηκευτικό χώρο, και είναι πολύ πιο χρήσιμο να τα έχουμε ενεργοποιημένα. Επίσης δεν φαίνεται να προκαλούν κάποια σημαντική καθυστέρηση ή επιβάρυνση. Με τα checksums ενεργοποιημένα, μπορούμε να ζητήσουμε από το ZFS να ελέγξει την ακεραιότητα των δεδομένων χρησιμοποιώντας τα για επαλήθευση. Η διαδικασία αυτή είναι γνωστή ως "scrubbing." Για να ελέγξετε την ακεραιότητα δεδομένων του pool `storage`, χρησιμοποιήστε την παρακάτω εντολή:

```
# zpool scrub storage
```

Η διαδικασία αυτή μπορεί να πάρει αρκετή ώρα, ανάλογα με την ποσότητα των αποθηκευμένων δεδομένων. Επίσης χρησιμοποιεί πάρα πολύ το δίσκο (I/O), τόσο ώστε σε κάθε δεδομένη στιγμή

μπορεί να εκτελείται μόνο μια τέτοια διαδικασία. Μετά την ολοκλήρωση του scrub, θα ανανεωθεί και η αναφορά κατάστασης, την οποία μπορείτε να δείτε ζητώντας την με την παρακάτω εντολή:

```
# zpool status storage
 pool: storage
 state: ONLINE
 scrub: scrub completed with 0 errors on Sat Aug 30 19:57:37 2008
config:

    NAME        STATE     READ WRITE CKSUM
    storage     ONLINE       0     0     0
      raidz1    ONLINE       0     0     0
        da0     ONLINE       0     0     0
        da1     ONLINE       0     0     0
        da2     ONLINE       0     0     0

errors: No known data errors
```

Στο παράδειγμα μας εμφανίζεται και η χρονική στιγμή που ολοκληρώθηκε η εντολή scrub. Η δυνατότητα αυτή μας εξασφαλίζει ακεραιότητα δεδομένων σε μεγάλο βάθος χρόνου.

Υπάρχουν πολλές ακόμα επιλογές για το σύστημα αρχείων Z. Δείτε τις σελίδες manual zfs(8) και zpool(8).

41.2.2.5. ZFS Quotas

Το ZFS υποστηρίζει διαφορετικούς τύπους quota: το refquota, το γενικό quota, το quota χρήστη και το quota ομάδας. Στην ενότητα αυτή θα εξηγήσουμε τις βασικές έννοιες κάθε τύπου και θα δώσουμε κάποιες οδηγίες χρήσης.

Τα quotas χρησιμοποιούνται για να περιορίσουν το χώρο στο δίσκο που μπορεί να καταναλωθεί από ένα dataset και τους απογόνους του (descendants) του καθώς και για να θέσουν περιορισμούς στο χώρο που μπορεί να καταλάβει ένα στιγμιότυπο (snapshot). Σε όρους χρήστη, τα quotas είναι χρήσιμα για τον περιορισμό του χώρου δίσκου που μπορεί να έχει στη διάθεση του κάποιος χρήστης.

Δεν μπορείτε να ορίσετε quotas σε τόμους (volumes) καθώς αυτό ουσιαστικά γίνεται ήδη από την ιδιότητα `volsize`.

Το refquota, `refquota=size`, περιορίζει το χώρο που μπορεί να καταναλώσει ένα dataset θέτοντας ένα απόλυτο όριο χώρου (hard limit). Ωστόσο, αυτό το απόλυτο όριο δεν περιλαμβάνει το χώρο που χρησιμοποιείται από τους απογόνους του dataset όπως τα συστήματα αρχείων ή τα στιγμιότυπα.

Για να επιβάλετε γενικό quota 10 GB για το storage/home/bob, χρησιμοποιήστε την παρακάτω εντολή:

```
# zfs set quota=10G storage/home/bob
```

Τα quotas χρήστη περιορίζουν την ποσότητα χώρου που μπορεί να χρησιμοποιήσει ένας συγκεκριμένος χρήστης. Η γενική μορφή είναι `userquota@user=size`, και το όνομα του χρήστη πρέπει να δίνεται σε μια από τις παρακάτω μορφές:

- Μορφή συμβατή με το POSIX, για παράδειγμα *joe*.
- Μορφή συμβατή με το αριθμητικό αναγνωριστικό (ID) του POSIX, για παράδειγμα *789*.
- Μορφή ονόματος SID, για παράδειγμα *joe.bloggs@example.com*.
- Μορφή αριθμητικού αναγνωριστικού (ID) SID, για παράδειγμα *S-1-123-456-789*.

Για παράδειγμα, για να επιβάλετε quota 50 GB για ένα χρήστη με όνομα *joe*, χρησιμοποιήστε την παρακάτω εντολή:

```
# zfs set userquota@joe=50G
```

Για να αφαιρέσετε το quota ή να βεβαιωθείτε ότι δεν έχει τεθεί, χρησιμοποιήστε την εντολή:

```
# zfs set userquota@joe=none
```

Οι ιδιότητες των quota χρηστών δεν απεικονίζονται μέσω της εντολής `zfs get all`. Οι χρήστες εκτός του `root` μπορούν να δουν μόνο τα δικά τους quotas εκτός αν τους έχει αποδοθεί το προνόμιο `userquota`. Οι χρήστες με αυτό το προνόμιο μπορούν να δουν και να ρυθμίσουν το quota οποιουδήποτε χρήστη.

Το quota ομάδας περιορίζει το διαθέσιμο χώρο που μπορεί να χρησιμοποιηθεί από μια συγκεκριμένη ομάδα χρηστών. Η γενική μορφή είναι `groupquota@group=size`.

Για να θέσετε quota για την ομάδα χρηστών *firstgroup* τα 50 GB, χρησιμοποιήστε την παρακάτω εντολή:

```
# zfs set groupquota@firstgroup=50G
```

Για να αφαιρέσετε το quota ή να βεβαιωθείτε ότι δεν έχει τεθεί, χρησιμοποιήστε την εντολή:

```
# zfs set groupquota@firstgroup=none
```

Όπως και με την ιδιότητα quota χρηστών, οι χρήστες εκτός του `root` μπορούν να δουν μόνο τα quota που σχετίζονται με τις ομάδες στις οποίες ανήκουν. Ωστόσο, ο χρήστης `root` και κάθε χρήστης στον οποίο έχει δοθεί το προνόμιο `groupquota` μπορεί να δει και να ρυθμίσει τα quota για όλες τις ομάδες.

Η υπο-εντολή `zfs userspace` απεικονίζει την ποσότητα χώρου που καταναλώνει κάθε χρήστης στο συγκεκριμένο σύστημα αρχείων ή στιγμιότυπο καθώς και το καθορισμένο quota. Η υπο-εντολή `zfs groupspace` εκτελεί ακριβώς το ίδιο για ομάδες χρηστών. Για περισσότερες πληροφορίες σχετικά με τις επιλογές εκτέλεσης ή απεικόνισης αυτών των εντολών, δείτε το zfs(1).

Για να δειτε το quota για το storage/home/bob, αν έχετε τα σωστά προνόμια ή είστε ο `root`, χρησιμοποιήστε την παρακάτω εντολή:

```
# zfs get quota storage/home/bob
```

41.2.2.6. Κρατήσεις Χώρου (reservations) στο ZFS

Το ZFS υποστηρίζει δύο τύπους κρατήσεων χώρου. Σε αυτή την ενότητα θα εξηγήσουμε τις βασικές έννοιες κάθε τύπο και θα δώσουμε κάποιες οδηγίες χρήσης.

Η ιδιότητα `reservation` μας επιτρέπει να διαφυλάξουμε κάποιο εγγυημένο ελάχιστο ποσό χώρου για ένα dataset και τους απογόνους του. Αυτό σημαίνει ότι αν τεθεί κράτηση χώρου 10 GB στο storage/home/bob και ο διαθέσιμος χώρος του δίσκου καταστεί ελάχιστος, θα διαφυλαχθούν τουλάχιστον 10 GB χώρου για αυτό το dataset. Η ιδιότητα `refreservation` θέτει ή δείχνει την ελάχιστη ποσότητα χώρου που έχει κρατηθεί για ένα dataset χωρίς τους απογόνους του (π.χ. τα στιγμιότυπα). Για παράδειγμα, για να πάρετε ένα στιγμιότυπο του storage/home/bob θα πρέπει να έχετε επαρκή χώρο εκτός της ποσότητας `refreservation` για να εκτελέσετε επιτυχώς τη λειτουργία. Οι απόγονοι του κυρίου dataset δεν προσμετρώνται από την ιδιότητα `refreservation` και δεν καταπατούν τον ελεύθερο χώρο του.

Οι κρατήσεις κάθε τύπου είναι χρήσιμες σε πολλές περιπτώσεις, για παράδειγμα στο σχεδιασμό και δοκιμή καταλληλότητας της κατανομής χώρου σε ένα νέο σύστημα ή την εξασφάλιση διαθεσιμότητας αρκετού ελεύθερου χώρου σε ένα σύστημα για λειτουργίες ανάκτησης δεδομένων (recovery).

Η γενική μορφή της ιδιότητας `reservation` είναι `reservation=size`. Για να θέσετε κράτηση 10 GB στο storage/home/bob χρησιμοποιήστε την παρακάτω εντολή:

```
# zfs set reservation=10G storage/home/bob
```

Για να αφαιρέσετε ένα reservation ή να βεβαιωθείτε ότι δεν έχει τεθεί, εκτελέστε την εντολή:

```
# zfs set reservation=none storage/home/bob
```

Μπορείτε να εφαρμόσετε την ίδια βασική αρχή και για να θέσετε την ιδιότητα `refreservation`, χρησιμοποιώντας τη γενική μορφή `refreservation=size`.

Για να ελέγξετε αν υπάρχουν reservations ή refreservations στο storage/home/bob, εκτελέστε μια από τις παρακάτω εντολές:

```
# zfs get reservation storage/home/bob
# zfs get refreservation storage/home/bob
```

41.3. Συστήματα Αρχείων Linux®

Αυτή η ενότητα περιγράφει κάποια από τα συστήματα αρχείων του Linux® που υποστηρίζονται από το FreeBSD.

41.3.1. Ext2FS

Η υλοποίηση του συστήματος αρχείων ext2fs(5) στον πυρήνα, γράφηκε από τον Godmar Back και το πρόγραμμα οδήγησης εμφανίστηκε για πρώτη φορά στο FreeBSD 2.2. Στο FreeBSD 8 και στις προηγούμενες εκδόσεις, ο κώδικας ήταν υπό την άδεια GNU Public License, ωστόσο στο FreeBSD 9 ο κώδικας γράφτηκε ξανά και είναι πλέον υπό την άδεια BSD.

Το πρόγραμμα οδήγησης ext2fs(5) επιτρέπει στον πυρήνα του FreeBSD τόσο να διαβάζει όσο και να γράφει σε συστήματα αρχείων ext2.

Αρχικά, φορτώστε το άρθρωμα στον πυρήνα:

```
# kldload ext2fs
```

Για να προσαρτήσετε έπειτα ένα τόμο ext2fs(5) που βρίσκεται στο /dev/ad1s1:

```
# mount -t ext2fs /dev/ad1s1 /mnt
```

41.3.2. XFS

Το σύστημα αρχείων X, XFS γράφτηκε αρχικά από την SGI για το λειτουργικό IRIX και μεταφέρθηκε στο Linux®. Ο πηγαίος κώδικας είναι διαθέσιμος υπό την άδεια GNU Public License. Δείτε αυτή τη σελίδα για περισσότερες πληροφορίες. Η μεταφορά στο FreeBSD ξεκίνησε από τους Russel Cattelan, Alexander Kabaev <kan@FreeBSD.org> και Craig Rodrigues <rodrigc@FreeBSD.org>.

Για να φορτώσετε το XFS ως άρθρωμα στον πυρήνα:

```
# kldload xfs
```

Το πρόγραμμα οδήγησης xfs(5) επιτρέπει στον πυρήνα του FreeBSD να έχει πρόσβαση σε συστήματα αρχείων XFS. Ωστόσο, τη δεδομένη στιγμή, επιτρέπει πρόσβαση μόνο για ανάγνωση. Η εγγραφή δεν είναι δυνατή.

Για να προσαρτήσετε ένα τόμο xfs(5) που βρίσκεται στο /dev/ad1s1, εκτελέστε την παρακάτω εντολή:

```
# mount -t xfs /dev/ad1s1 /mnt
```

Καλό είναι επίσης να γνωρίζετε ότι το port sysutils/xfsprogs περιέχει το βοηθητικό πρόγραμμα `mkfs.xfs` το οποίο επιτρέπει τη δημιουργία συστημάτων αρχείων XFS. Το port επίσης παρέχει

προγράμματα για έλεγχο και επισκευή αυτών των συστημάτων αρχείων.

Μπορείτε να χρησιμοποίησετε την παράμετρο `-p` στην εντολή `mkfs.xfs` για να δημιουργήσετε ένα σύστημα αρχείων xfs(5) το οποίο να περιέχει αρχεία και άλλα μετα-δεδομένα. Με αυτό τον τρόπο μπορείτε να δημιουργήσετε ένα σύστημα αρχείων μόνο ανάγνωσης για δοκιμή με το FreeBSD.

41.3.3. ReiserFS

Το σύστημα αρχείων Reiser, ReiserFS, μεταφέρθηκε στο FreeBSD από τον Jean-Sébastien Pédron <dumbbell@FreeBSD.org> και είναι υπό την άδεια GNU Public License.

Το πρόγραμμα οδήγησης για το ReiserFS επιτρέπει στον πυρήνα του FreeBSD να έχει πρόσβαση ανάγνωσης στα αντίστοιχα συστήματα αρχείων αλλά τη δεδομένη στιγμή δεν επιτρέπει εγγραφή δεδομένων.

Φορτώστε αρχικά το άρθρωμα του πυρήνα:

```
# kldload reiserfs
```

Για να προσαρτήσετε ένα τόμο ReiserFS από το /dev/ad1s1:

```
# mount -t reiserfs /dev/ad1s1 /mnt
```

Chapter 42. Εικονικοποίηση

42.1. Σύνοψη

Το λογισμικό εικονικοποίησης επιτρέπει σε πολλαπλά λειτουργικά συστήματα να εκτελούνται ταυτόχρονα στον ίδιο υπολογιστή. Σε υπολογιστές PC το λογισμικό αυτό τυπικά χρησιμοποιεί ένα λειτουργικό ως ξενιστή (host) στο οποίο και εκτελείται, και το οποίο υποστηρίζει ένα οποιοδήποτε αριθμό από φιλοξενούμενα (guest) λειτουργικά.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τη διαφορά μεταξύ ενός ξενιστή (host) και ενός φιλοξενούμενου (guest) λειτουργικού.
- Πως να εγκαταστήσετε το FreeBSD σε ένα Apple® Macintosh® υπολογιστή που βασίζεται σε Intel® αρχιτεκτονική.
- Πώς να εγκαταστήσετε το FreeBSD κάτω από Microsoft® Windows® με το Virtual PC.
- Πως να βελτιστοποιήσετε ένα FreeBSD σύστημα για την καλύτερη απόδοση σε περιβάλλον εικονικού μηχανήματος.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να έχετε κατανοήσει τις βασικές έννοιες του UNIX® και του FreeBSD (Βασικές Έννοιες στο UNIX®).
- Να γνωρίζετε πως θα εγκαταστήσετε το FreeBSD (Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων).
- Να γνωρίζετε πως θα ρυθμίσετε τη σύνδεση σας στο δίκτυο (Προχωρημένα Θέματα Δικτύωσης).
- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

42.2. Το FreeBSD ως φιλοξενούμενο λειτουργικό

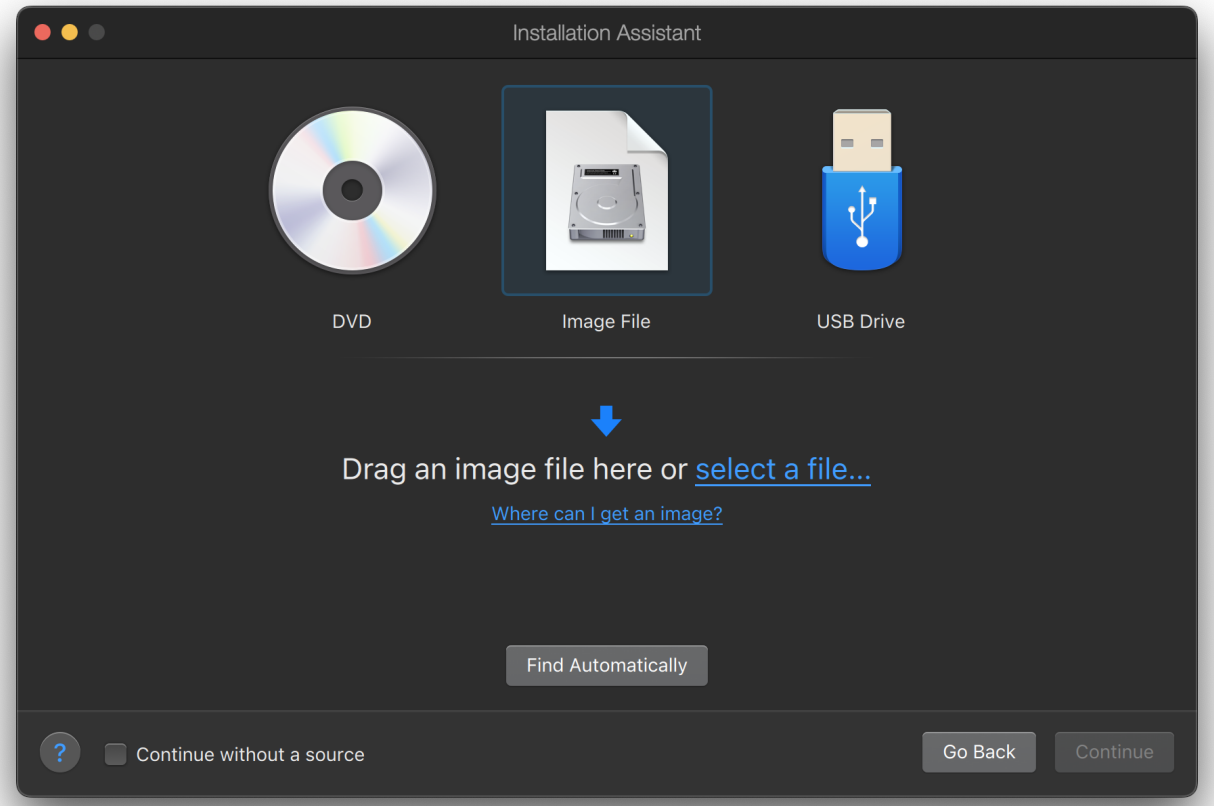
42.2.1. Το Parallels σε MacOS

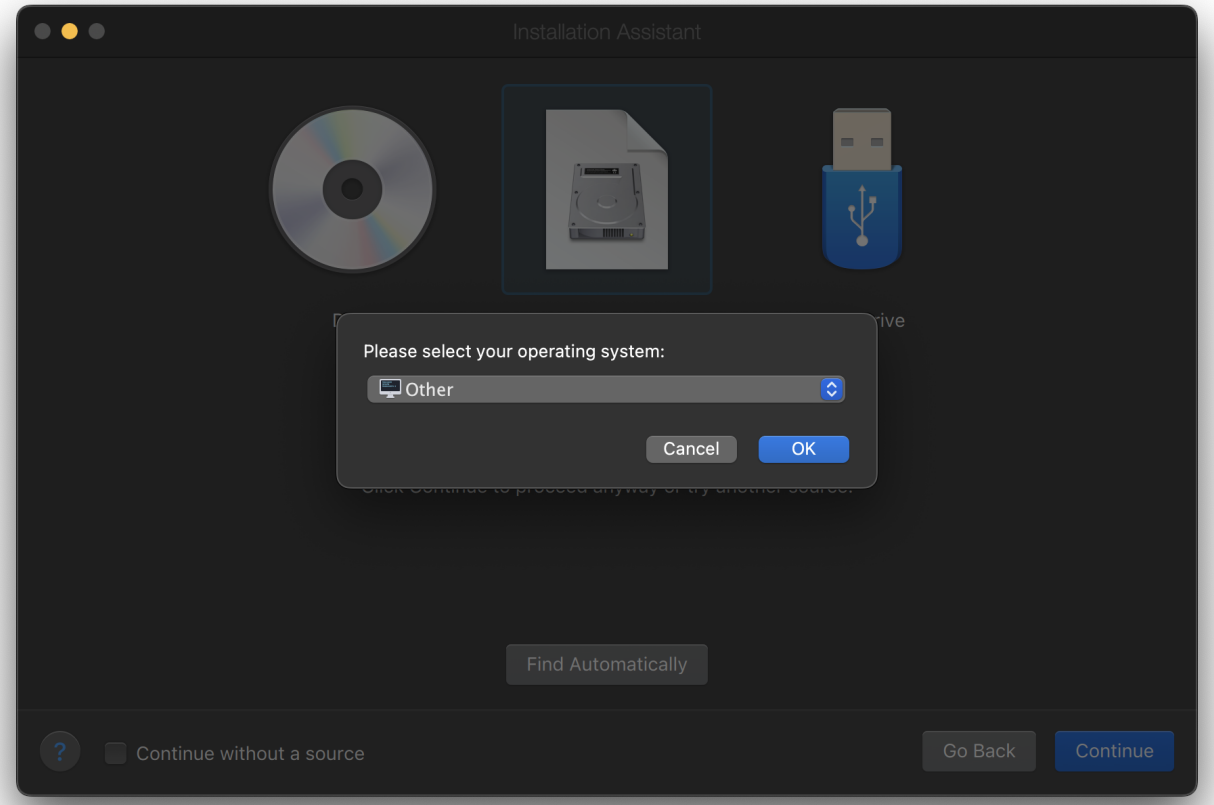
Το Parallels Desktop για Mac® είναι ένα εμπορικό λογισμικό το οποίον είναι διαθέσιμο για υπολογιστές Apple® Mac® με επεξεργαστή Intel® και λειτουργικό Mac OS® 10.4.6 ή νεότερο. Το FreeBSD παρέχει πλήρη υποστήριξη ως φιλοξενούμενο λειτουργικό. Όταν το Parallels έχει εγκατασταθεί στο Mac OS® X, ο χρήστης πρέπει να ρυθμίσει ένα εικονικό σύστημα και στη συνέχεια να εγκαταστήσει το φιλοξενούμενο λειτουργικό σύστημα που επιθυμεί.

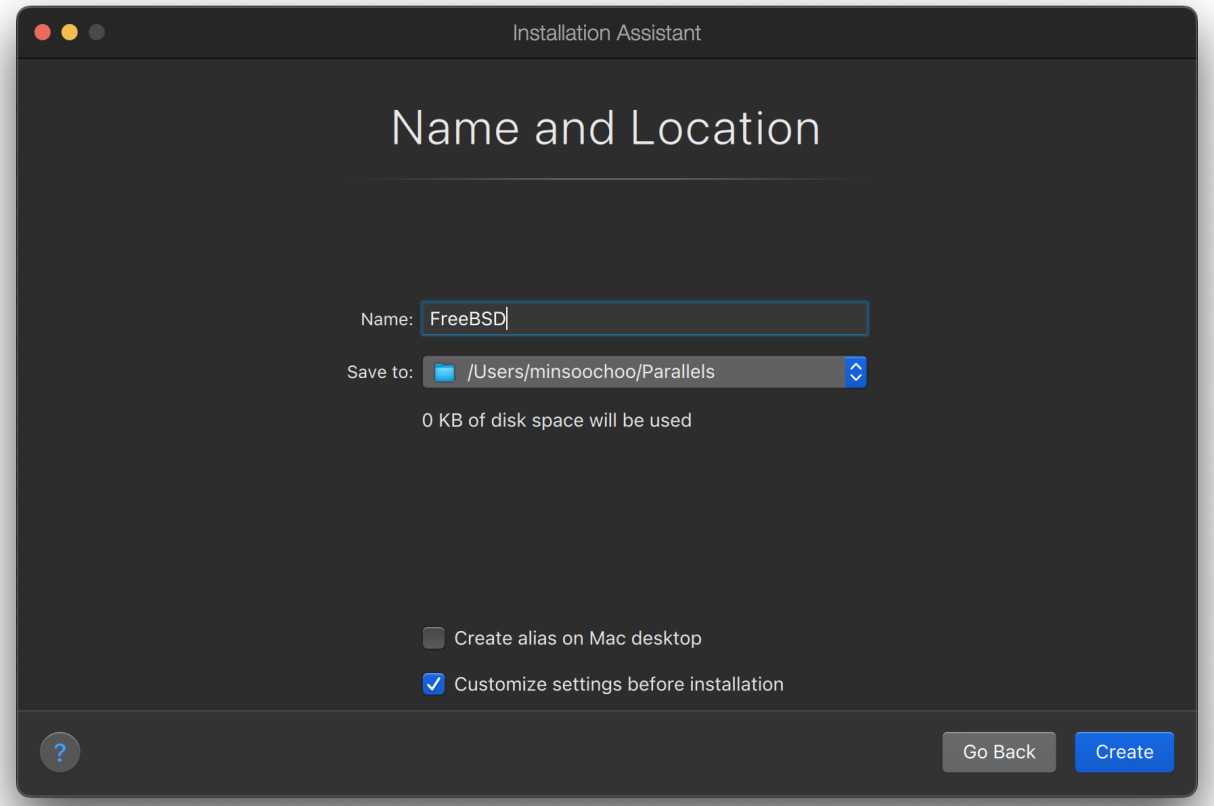
42.2.1.1. Εγκαθιστώντας το FreeBSD στο Parallels/Mac OS® X

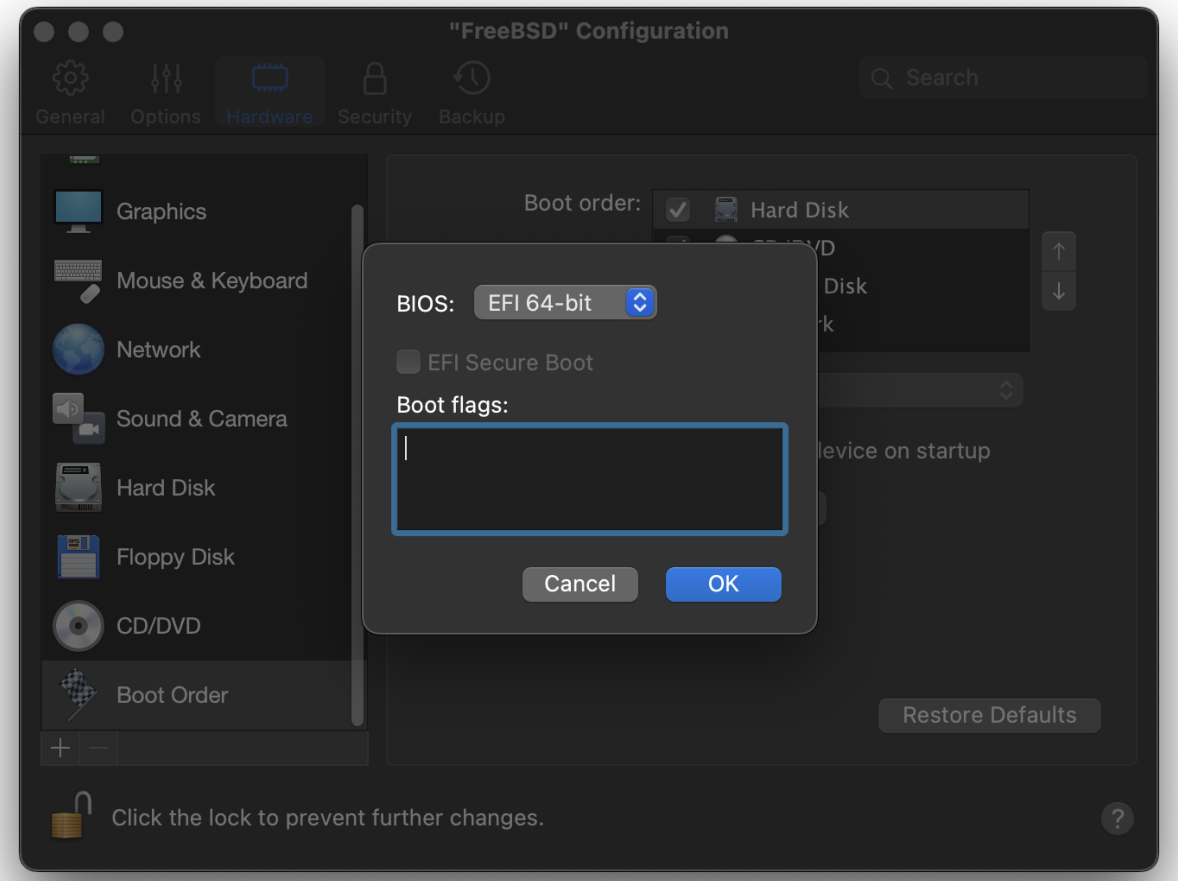
Το πρώτο βήμα για την εγκατάσταση του FreeBSD στο Mac OS® X/Parallels είναι να δημιουργήσετε ένα νέο εικονικό σύστημα για το FreeBSD. Όταν ερωτηθείτε, επιλέξτε το FreeBSD σαν το **φιλοξενούμενο λειτουργικό (Guest OS)**.

Ορίστε ένα λογικό μέγεθος δίσκου και μνήμης που να ανταποκρίνεται στα σχέδια που έχετε για την εικονικοποίηση του FreeBSD. 4GB δίσκος και 512MB μνήμης δουλεύουν μια χαρά για τους περισσότερους χρήστες του FreeBSDμέσα από το Parallels:

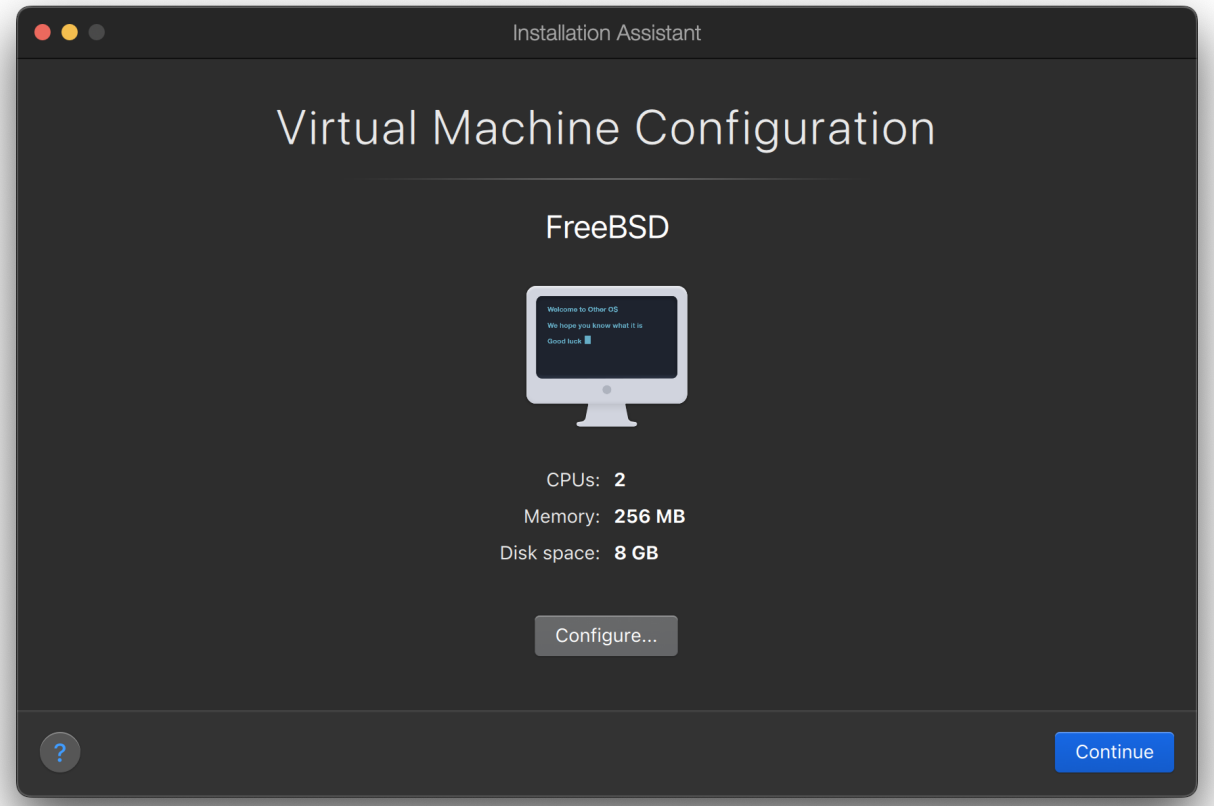

Installation Assistant
DVD
Image File
USB Drive
Drag an image file here or select a file...
Where can I get an image?
Find Automatically
Continue without a source
Go Back
Continue


Installation Assistant
Please select your operating system:
Other
Cancel
OK
Find Automatically
Continue without a source
Go Back
Continue

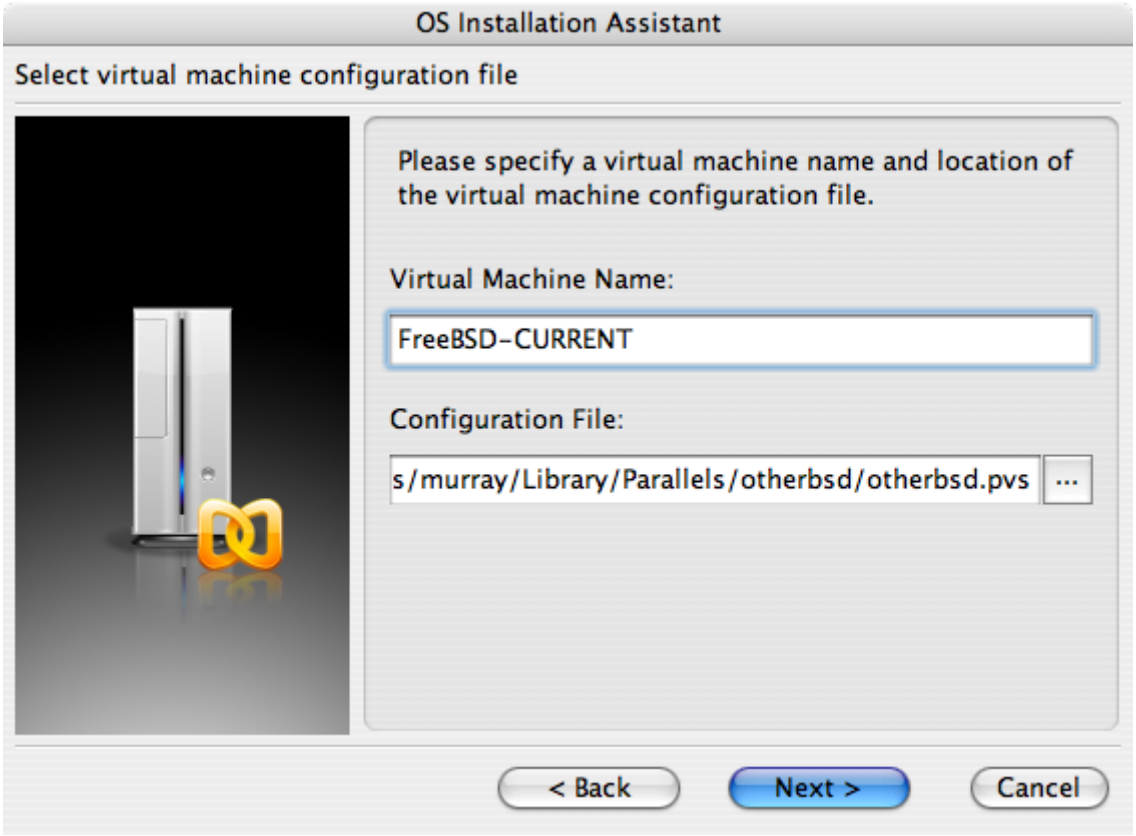

Installation Assistant
Name and Location
Name: FreeBSD
Save to: /Users/minsoochoo/Parallels
0 KB of disk space will be used
Create alias on Mac desktop
Customize settings before installation
Go Back
Create



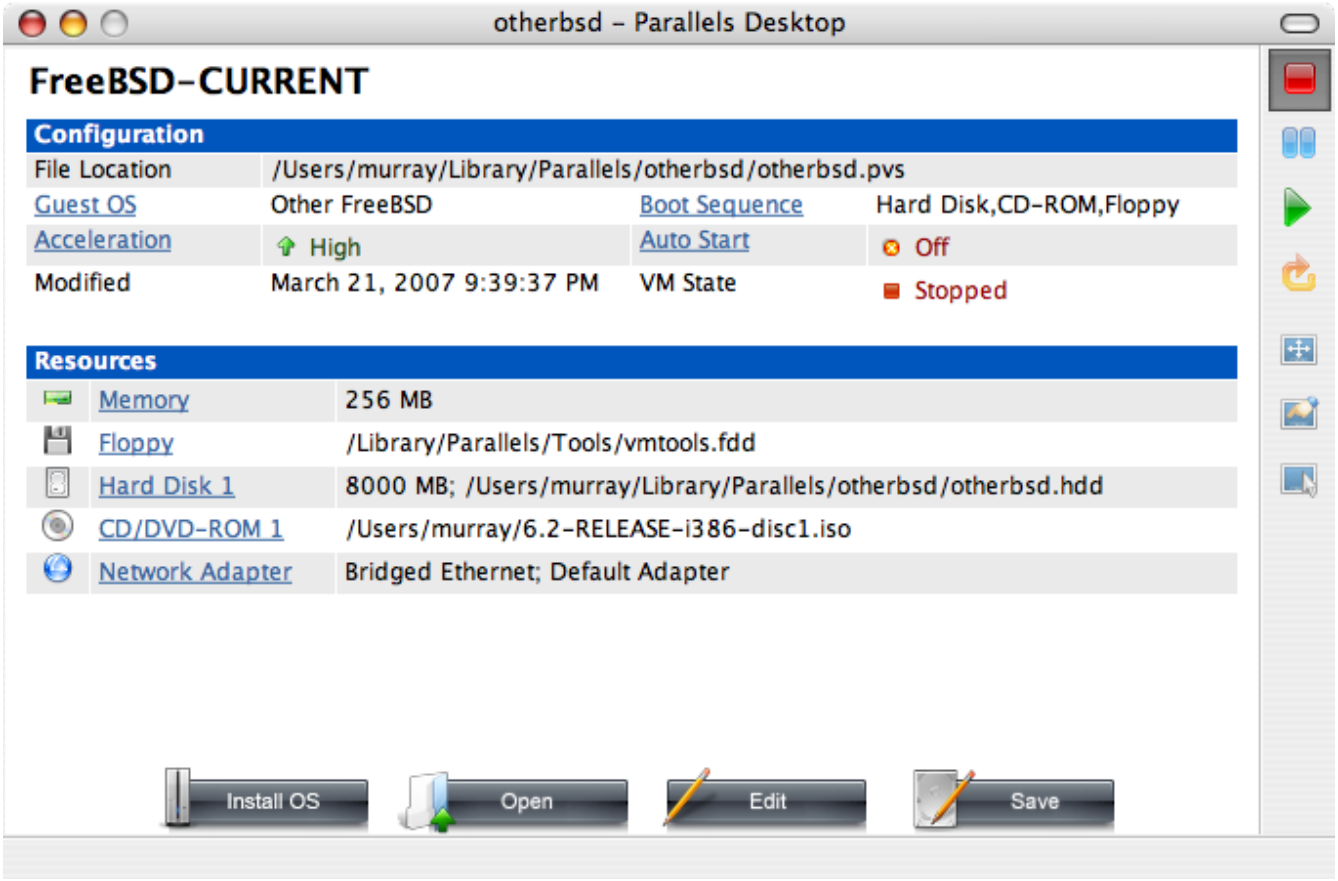
Επιλέξτε τον τύπο δικτύωσης και τον προσαρμογέα δικτύου:


Installation Assistant
Virtual Machine Configuration
FreeBSD
Welcome to Other OS
We hope you know what it is
Good luck
CPUs: 2
Memory: 256 MB
Disk space: 8 GB
Configure...
Continue

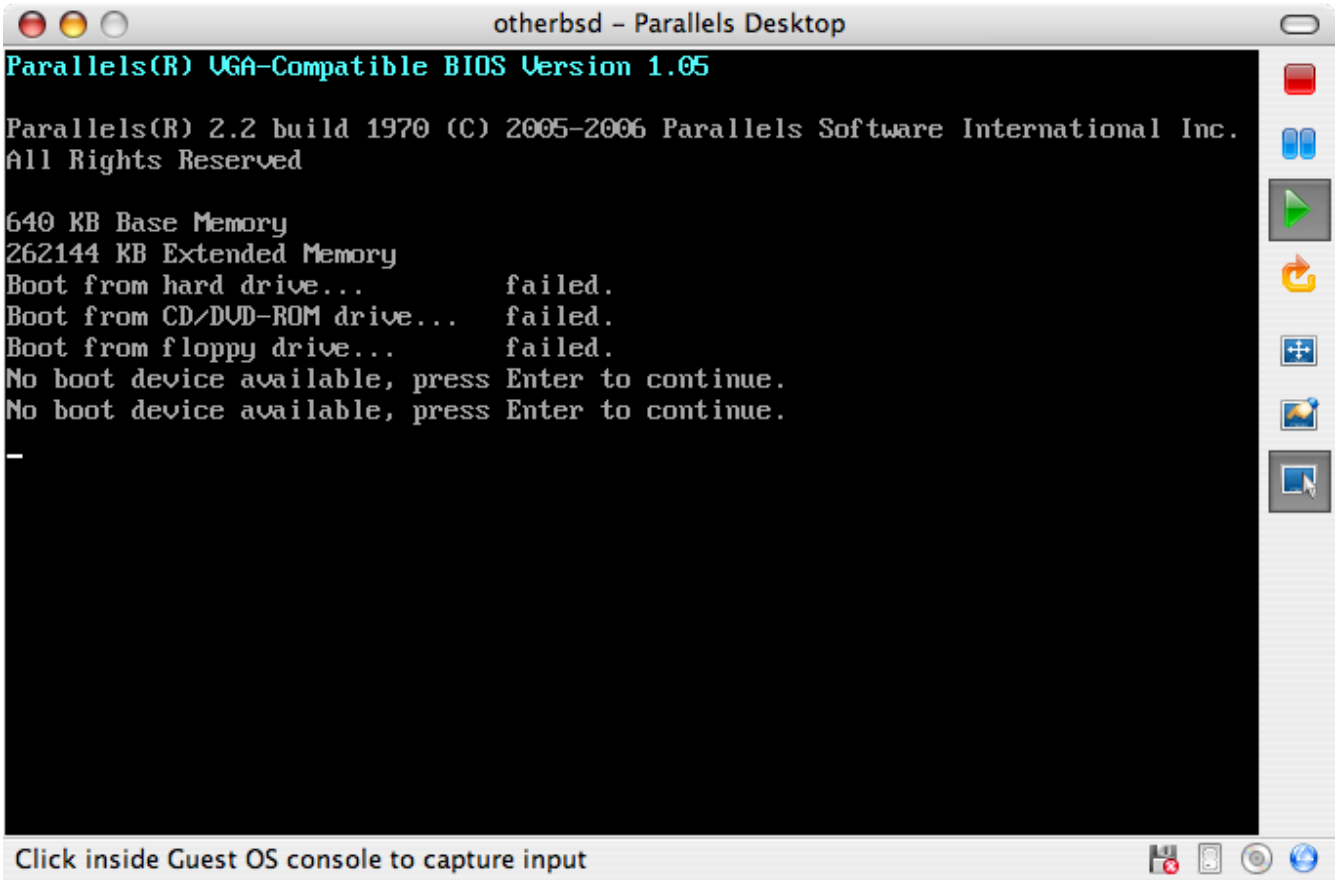
Αποθήκευση και τέλος των ρυθμίσεων:



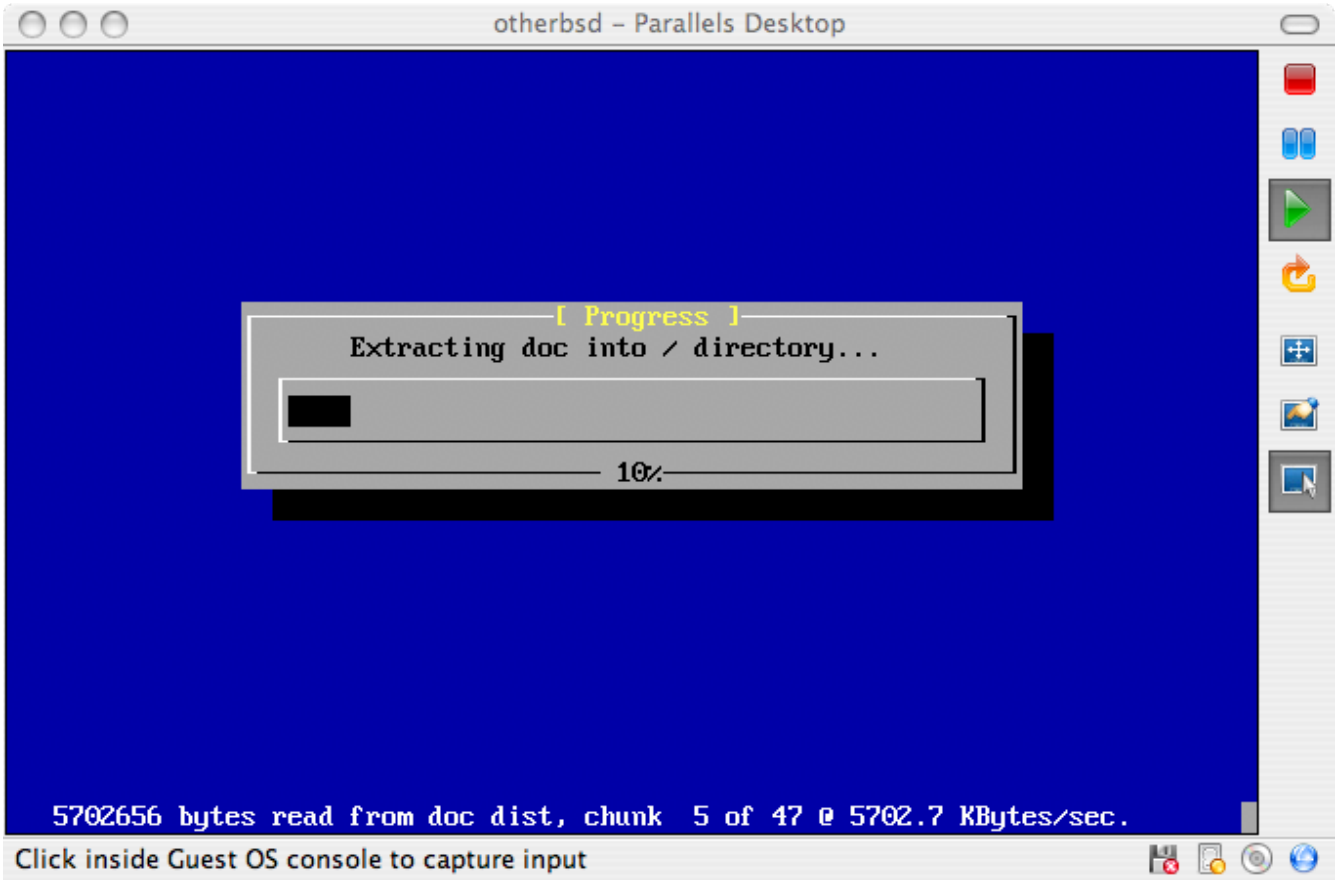
Όταν το εικονικό σύστημα έχει δημιουργηθεί, θα χρειαστεί να εγκαταστήσετε το ίδιο το FreeBSD. Ο καλύτερος τρόπος για να γίνει η εγκατάσταση είναι με το επίσημο FreeBSD CD-ROM ή με κάποιο αρχείο ISO, κατεβασμένο από τον επίσημο FTP τόπο. Όταν έχετε το κατάλληλο ISO στο σκληρό σας, ή το CD-ROM στον οδηγό CD, ενεργοποιήστε με το ποντίκι το εικονίδιο του CD στο κάτω δεξί μέρος της οθόνης του Parallels. Με αυτόν τον τρόπο θα μπορέσετε να ορίσετε την πηγή της εγκατάστασης. Μπορείτε να ορίσετε το CDROM ή κάποιο διαθέσιμο ISO αρχείο.



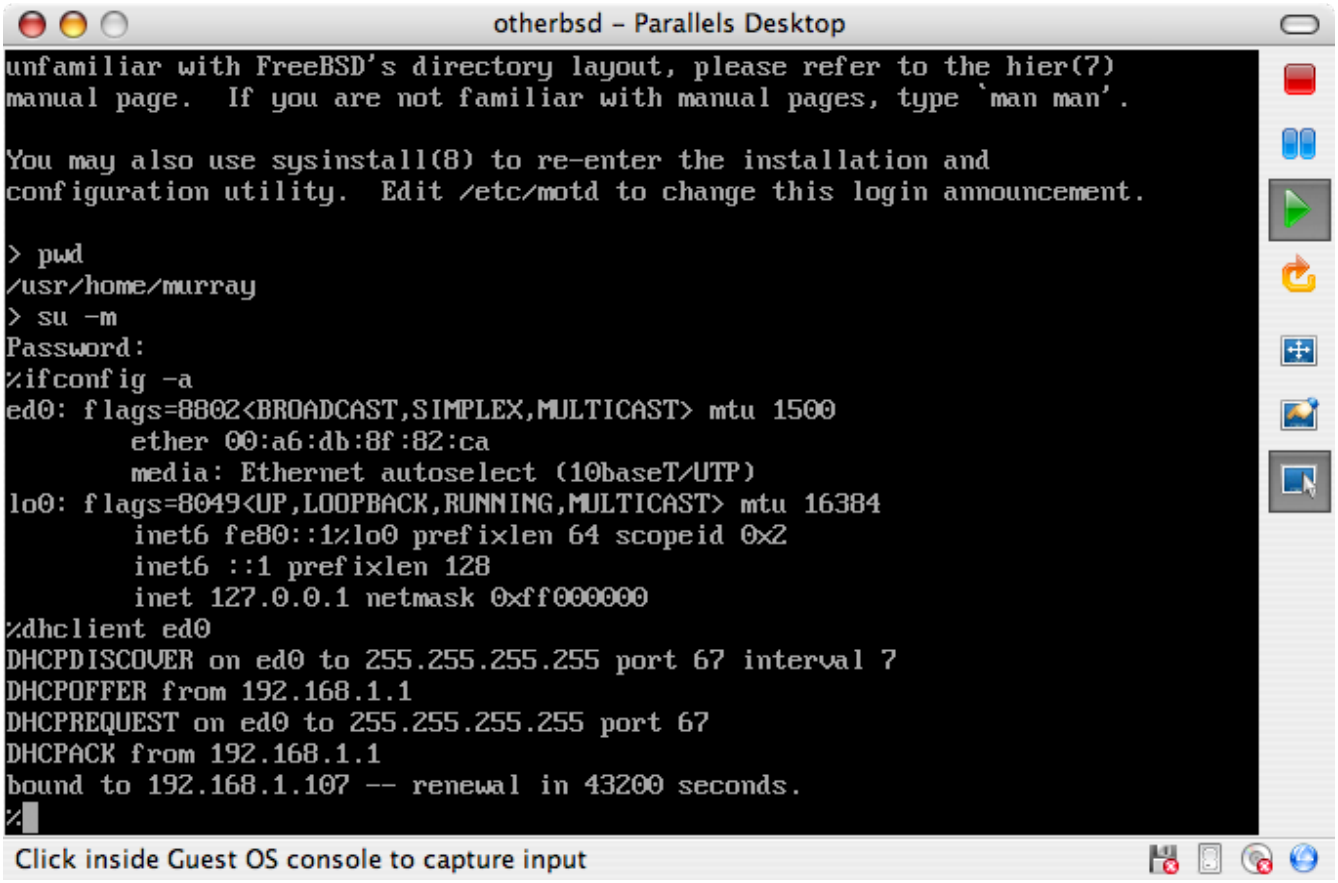
Όταν έχετε αντιστοιχήσει τη πηγή εγκατάστασης, επανεκκινήστε το εικονικό σύστημα πατώντας απλά το κουμπί της επανεκκίνησης (reboot) του Parallels. Το Parallels θα ξεκινήσει με ένα ειδικό BIOS το οποίο πρώτα ελέγχει εάν υπάρχει διαθέσιμο κάποιο CD-ROM, όπως κάνει και ένα φυσιολογικό BIOS.



Σε αυτή τη περίπτωση θα βρει το μέσο εγκατάστασης του FreeBSD και θα ξεκινήσει το sysinstall όπως περιγράφεται στο Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων. Μπορείτε να εγκαταστήσετε το X11, αλλά μη δοκιμάσετε να ρυθμίσετε αυτή τη στιγμή.



Όταν τελειώσετε με την εγκατάσταση, κάντε μια επανεκκίνηση στο φρέσκο εικονικό FreeBSD.



42.2.1.2. Ρυθμίζοντας το FreeBSD στο Mac OS® X/Parallels

Αφού έχει εγκατασταθεί επιτυχώς το FreeBSD στο Mac OS® X με το Parallels, υπάρχουν μερικά βήματα ακόμη που μπορούν να σας βοηθήσουν να ρυθμίσετε το εικονικό σας σύστημα.

1. Μεταβλητές του Boot Loader

   Το ποιο σημαντικό βήμα είναι να μειώσετε το μέγεθος του `kern.hz` προκειμένου να αξιοποιήσετε τη CPU μέσα από το Parallels. Αυτό μπορεί να γίνει με το να προσθέσετε την ακόλουθη γραμμή στο /boot/loader.conf:

   ```
   kern.hz=100
   ```

   Χωρίς αυτή τη ρύθμιση, ένα αδρανές FreeBSD στο Parallels θα καταναλώνει το 15% της CPU ενός μονοπύρηνου iMac®. Μετά από την αλλαγή, η κατανάλωση θα πέσει κοντά στο 5%.

2. Δημιουργία Νέου Αρχείου Ρυθμίσεων του Πυρήνα

   Μπορείτε να αφαιρέσετε όλες τους οδηγούς για SCSI, FireWire, και USB συσκευές. Το Parallels παρέχει ένα εικονικό προσαρμογέα δικτύου ο οποίος χρησιμοποιείται από τον οδηγό ed(4), οπότε όλοι οι οδηγοί για δικτυακές συσκευές εκτός των ed(4) και miibus(4) μπορούν να αφαιρεθούν από τον πυρήνα.

3. Ρύθμιση Δικτύου

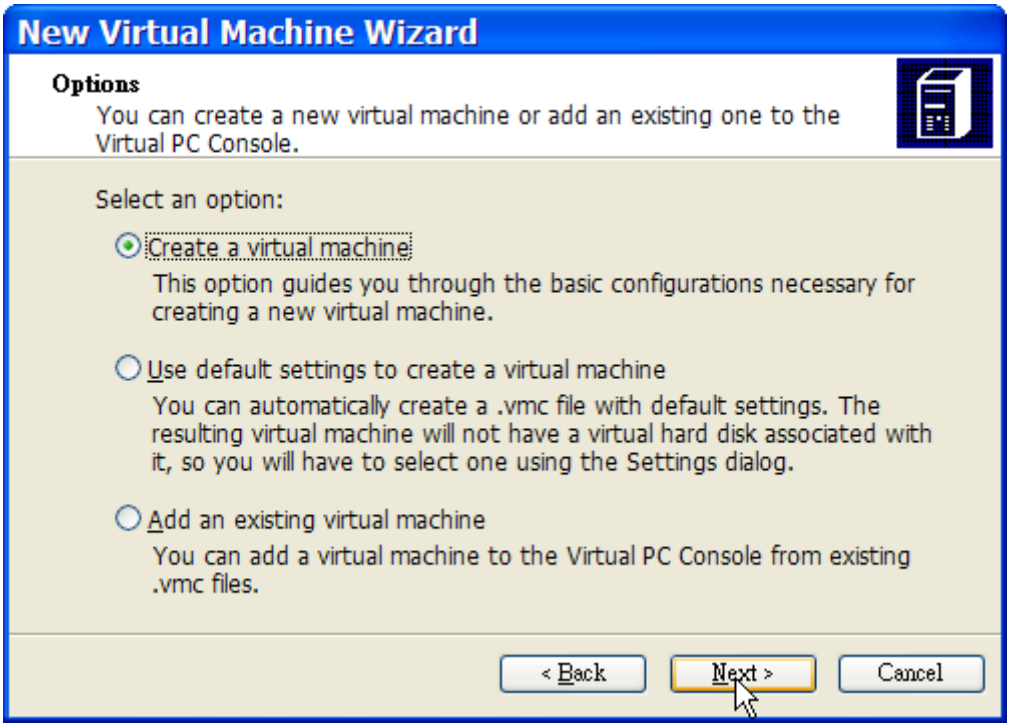
   Η πιο απλή ρύθμιση δικτύου κάνει χρήση του DHCP για να συνδεθεί το εικονικό σας σύστημα στο ίδιο τοπικό δίκτυο με τον Mac®. Αυτό μπορεί εύκολα να γίνει με το να προσθέσετε τη γραμμή `ifconfig_ed0="DHCP"` στο /etc/rc.conf. Πολυπλοκότερες ρυθμίσεις δικτύου περιγράφονται στο κεφάλαιο Προχωρημένα Θέματα Δικτύωσης.

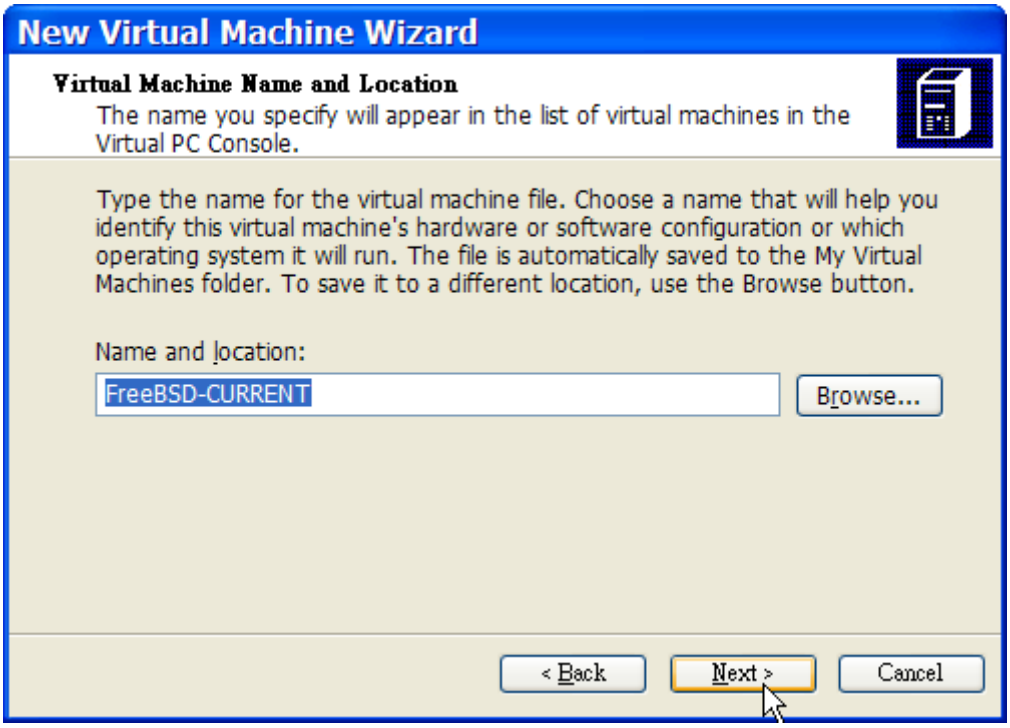
42.2.2. Το Virtual PC στα Windows®

Το Virtual PC για Windows® είναι ένα προϊόν της Microsoft® που διατίθεται για δωρεάν κατέβασμα. Δείτε τις απαιτήσεις συστήματος. Μετά την εγκατάσταση του Virtual PC στα Microsoft® Windows®, ο χρήστης πρέπει να ρυθμίσει ένα εικονικό μηχάνημα και να εγκαταστήσει το φιλοξενούμενο λειτουργικό που επιθυμεί.

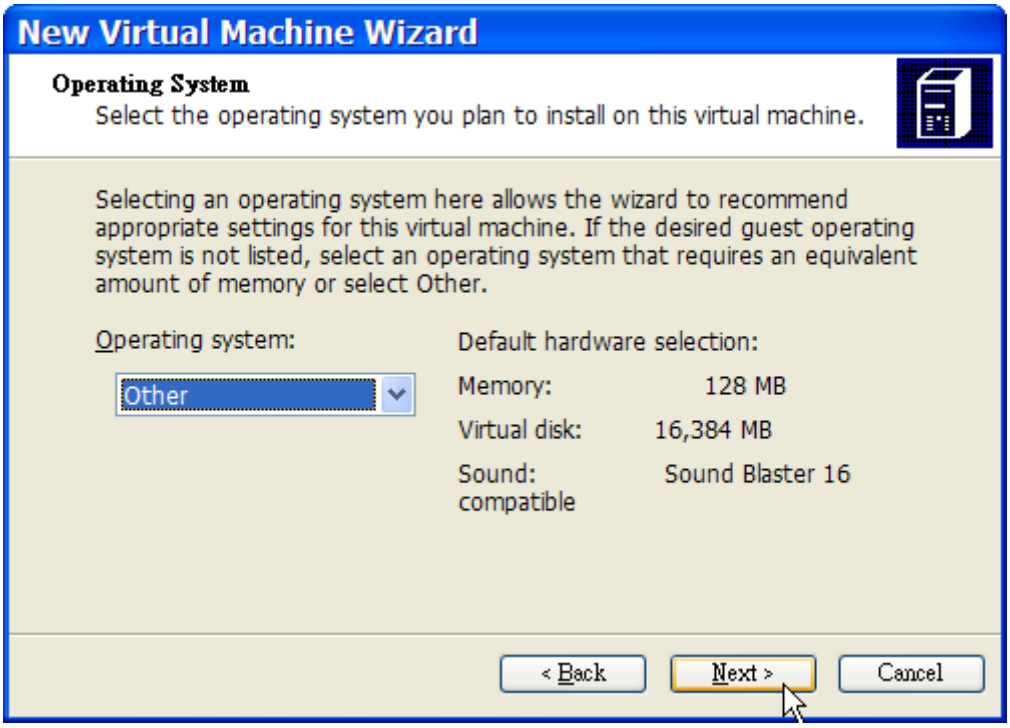
42.2.2.1. Εγκατάσταση του FreeBSD στο Virtual PC/Microsoft® Windows®

Το πρώτο βήμα στην εγκατάσταση του FreeBSD στα Microsoft® Windows® με χρήση του Virtual PC, είναι η δημιουργία ενός νέου εικονικού μηχανήματος για την εγκατάσταση του. Επιλέξτε Create a virtual machine όταν ερωτηθείτε:

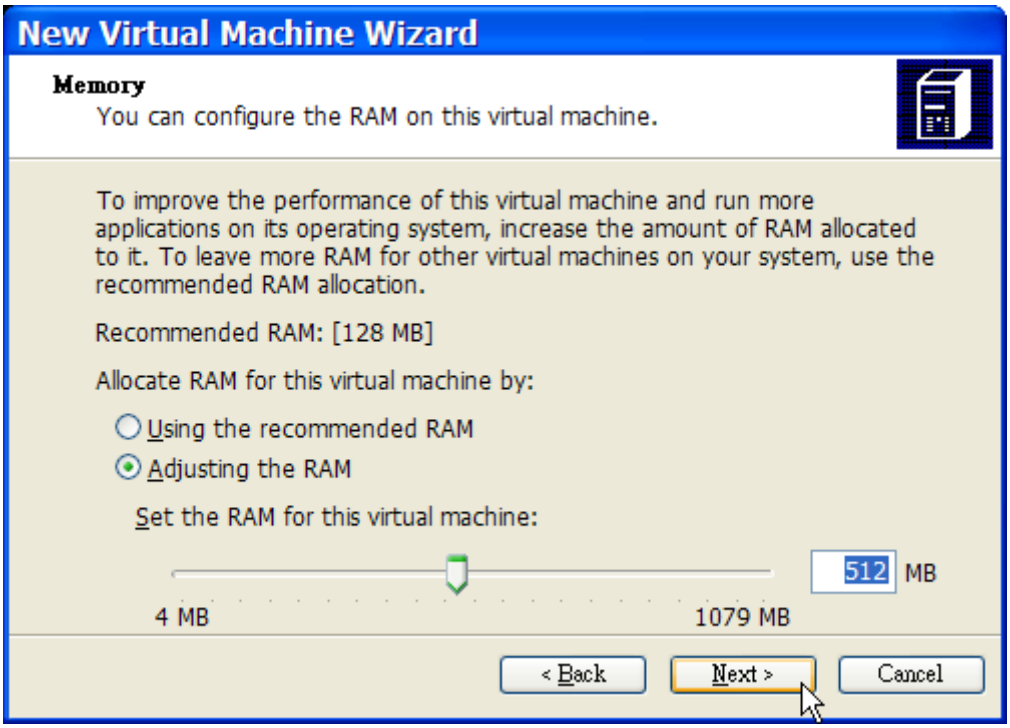


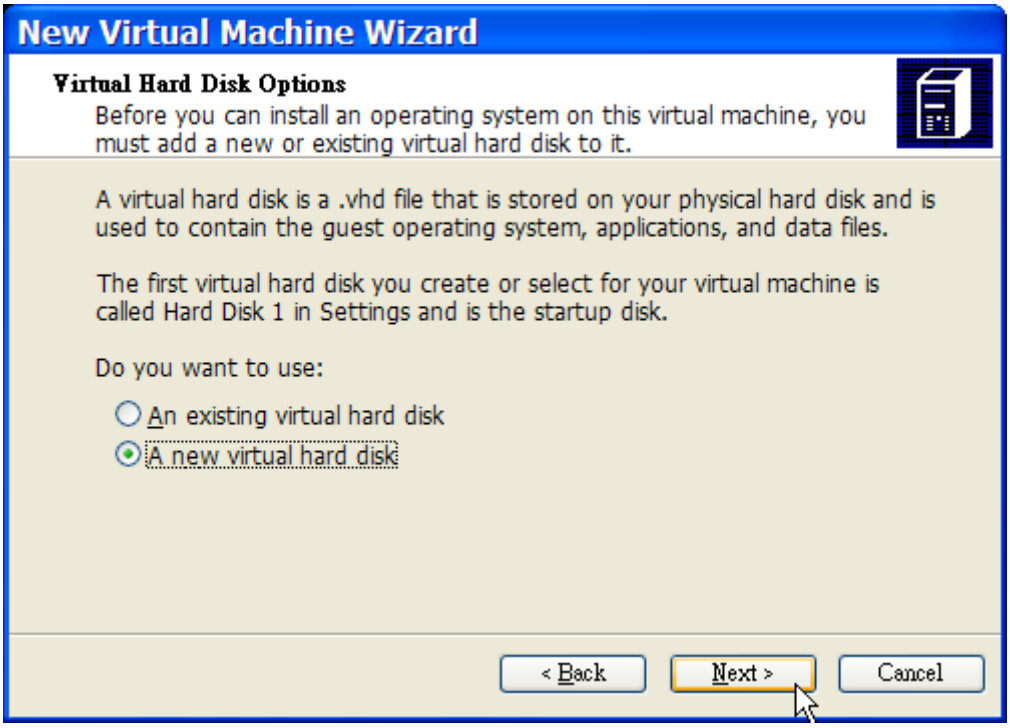


Στην ερώτηση Operating System επιλέξτε Other:

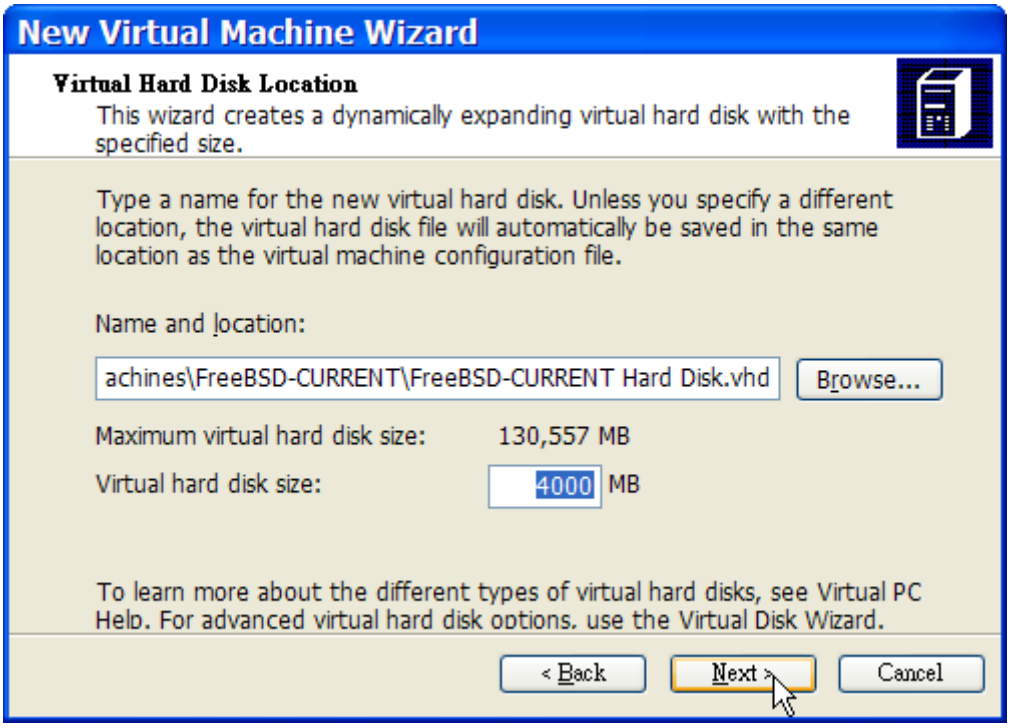


Επιλέξτε έπειτα κατάλληλο μέγεθος για το σκληρό δίσκο και τη μνήμη RAM του εικονικού μηχανήματος, ανάλογα με τη χρήση που σκοπεύετε να κάνετε. Στις περισσότερες περιπτώσεις, τα 4GB δίσκου και 512MB RAM είναι αρκετά για χρήση του FreeBSD στο Virtual PC:

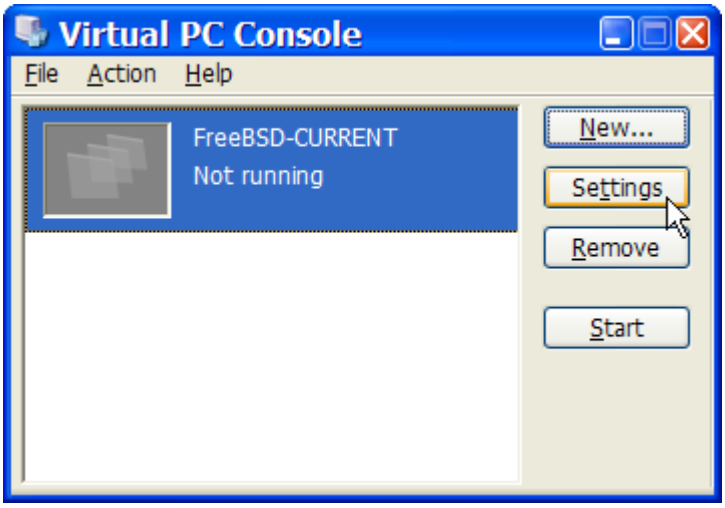


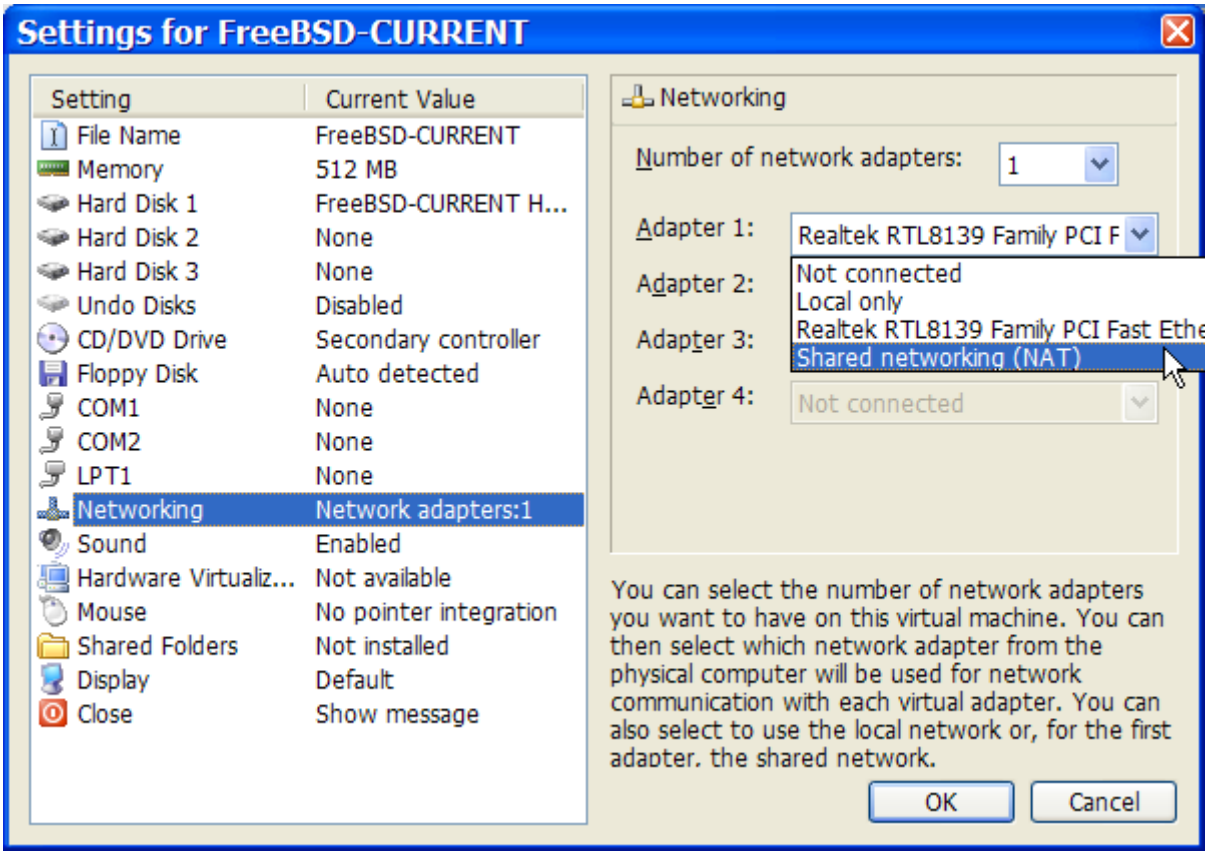


Ολοκληρώστε αποθηκεύοντας τις ρυθμίσεις:

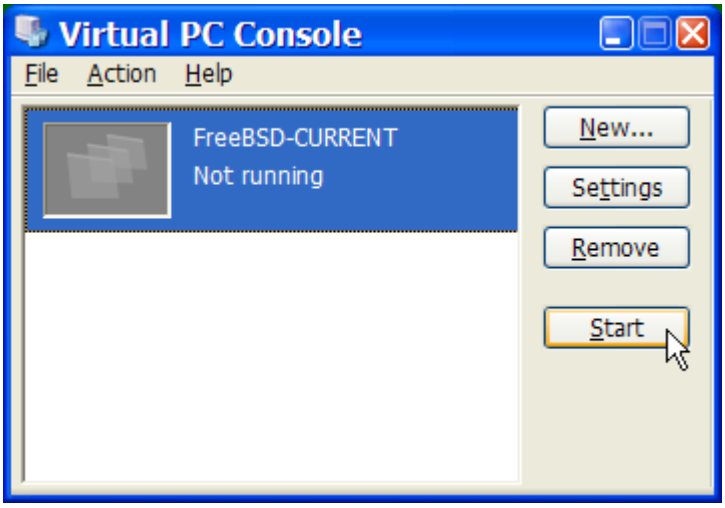


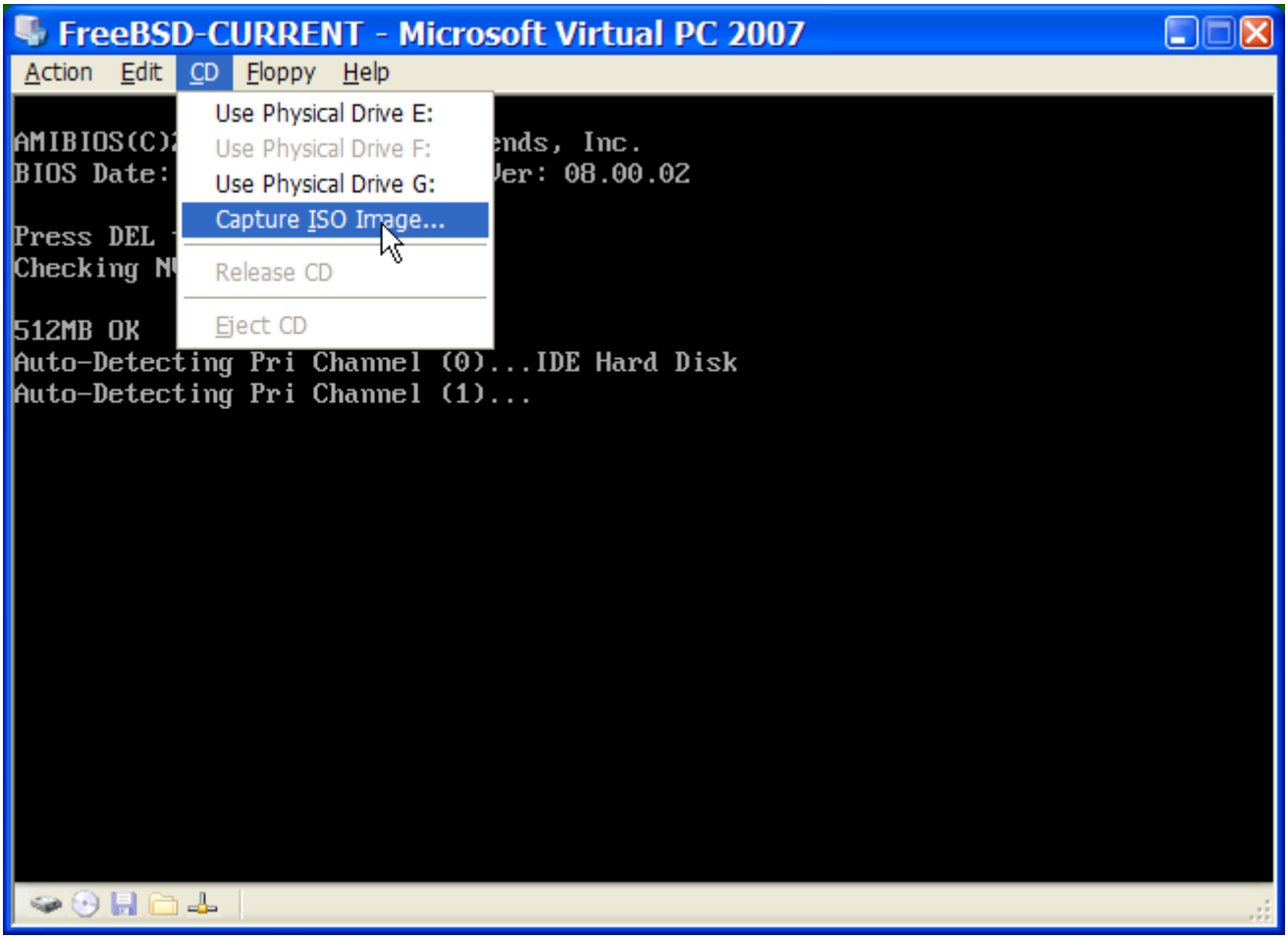
Επιλέξτε την εικονική μηχανή FreeBSD που δημιουργήσατε και κάντε κλικ στο Settings. Ρυθμίστε έπειτα το είδος και την διεπαφή (interface) του δικτύου:



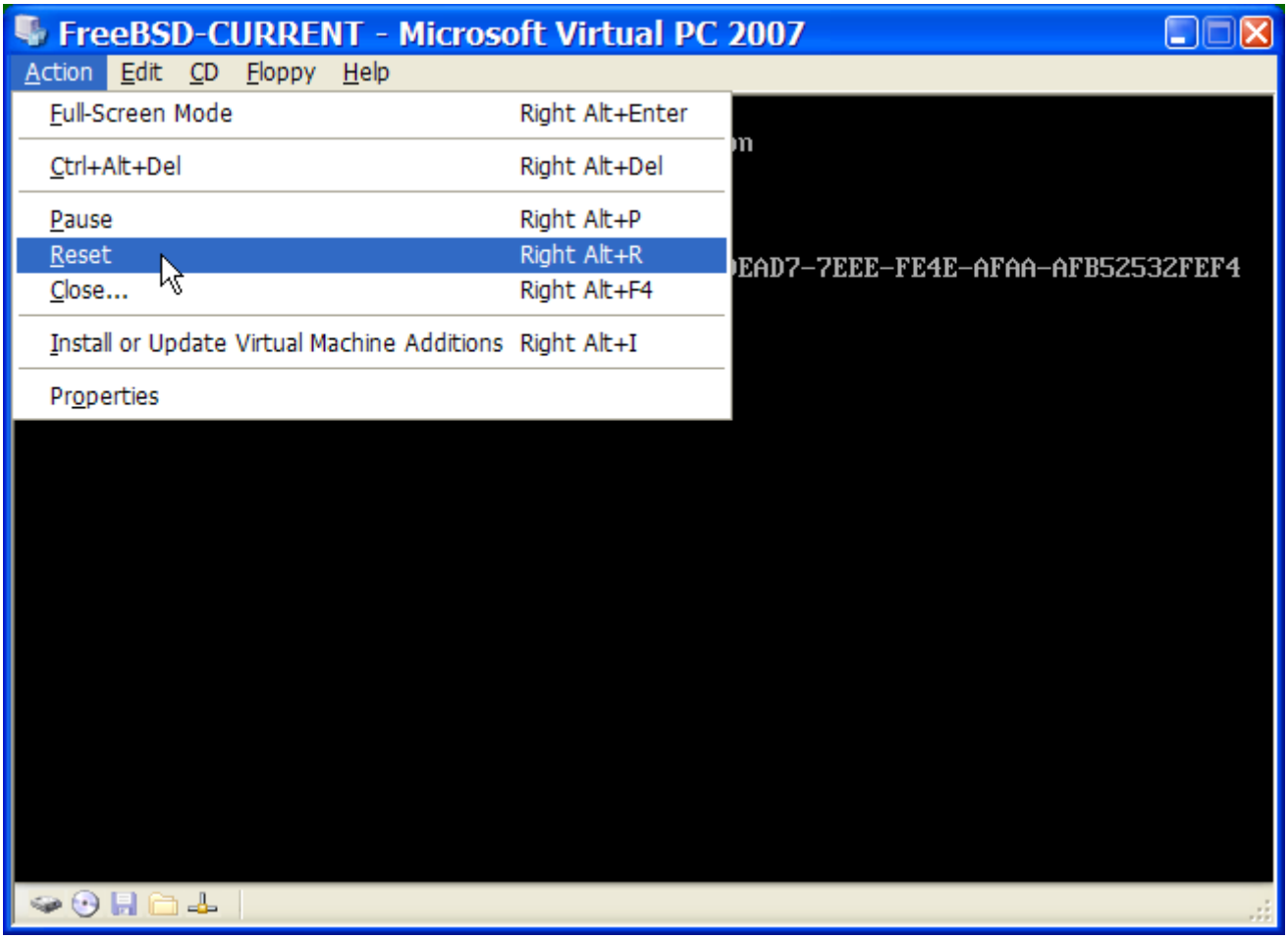


Αφού δημιουργήσετε την εικονική μηχανή σας για το FreeBSD, θα πρέπει να εγκαταστήσετε το λειτουργικό σε αυτήν. Ο καλύτερος τρόπος είναι να χρησιμοποιήσετε ένα από τα επίσημα CDROM του FreeBSD ή να κατεβάσετε κάποιο αρχείο ISO από την επίσημη τοποθεσία FTP. Έχοντας το κατάλληλο αρχείο ISO στο τοπικό σας σύστημα αρχείων των Windows® (ή το αντίστοιχο CDROM στον οδηγό), κάντε διπλό κλικ στο εικονίδιο της εικονικής μηχανής FreeBSD για να την εκκινήσετε. Έπειτα κάντε κλικ στο **CD** και επιλέξτε **Capture ISO Image...** στο παράθυρο του Virtual PC. Θα εμφανιστεί ένα παράθυρο που θα σας επιτρέψει να συσχετίσετε τον εικονικό οδηγό CDROM με ένα αρχείο ISO ή και με τον πραγματικό σας οδηγό.

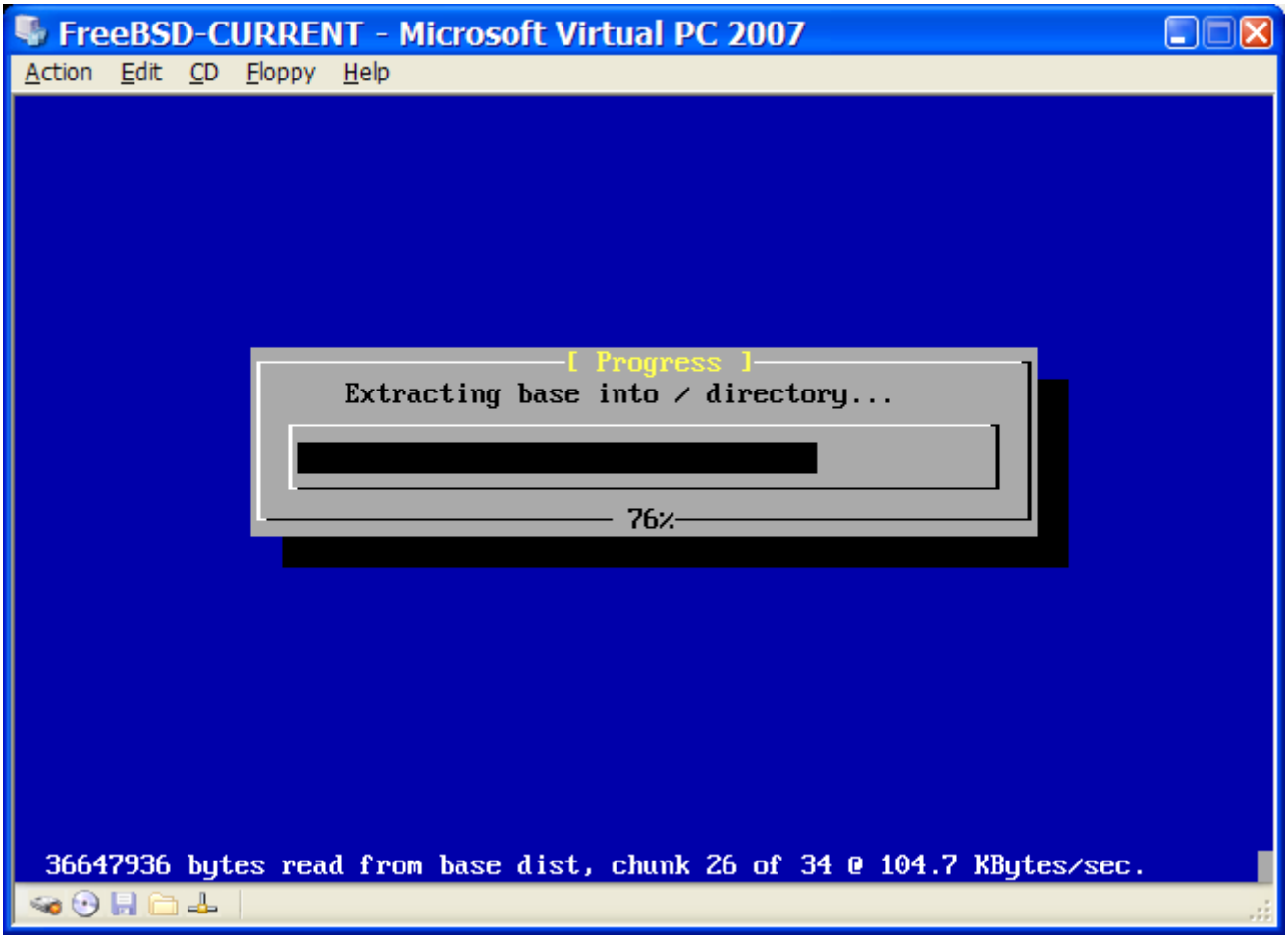




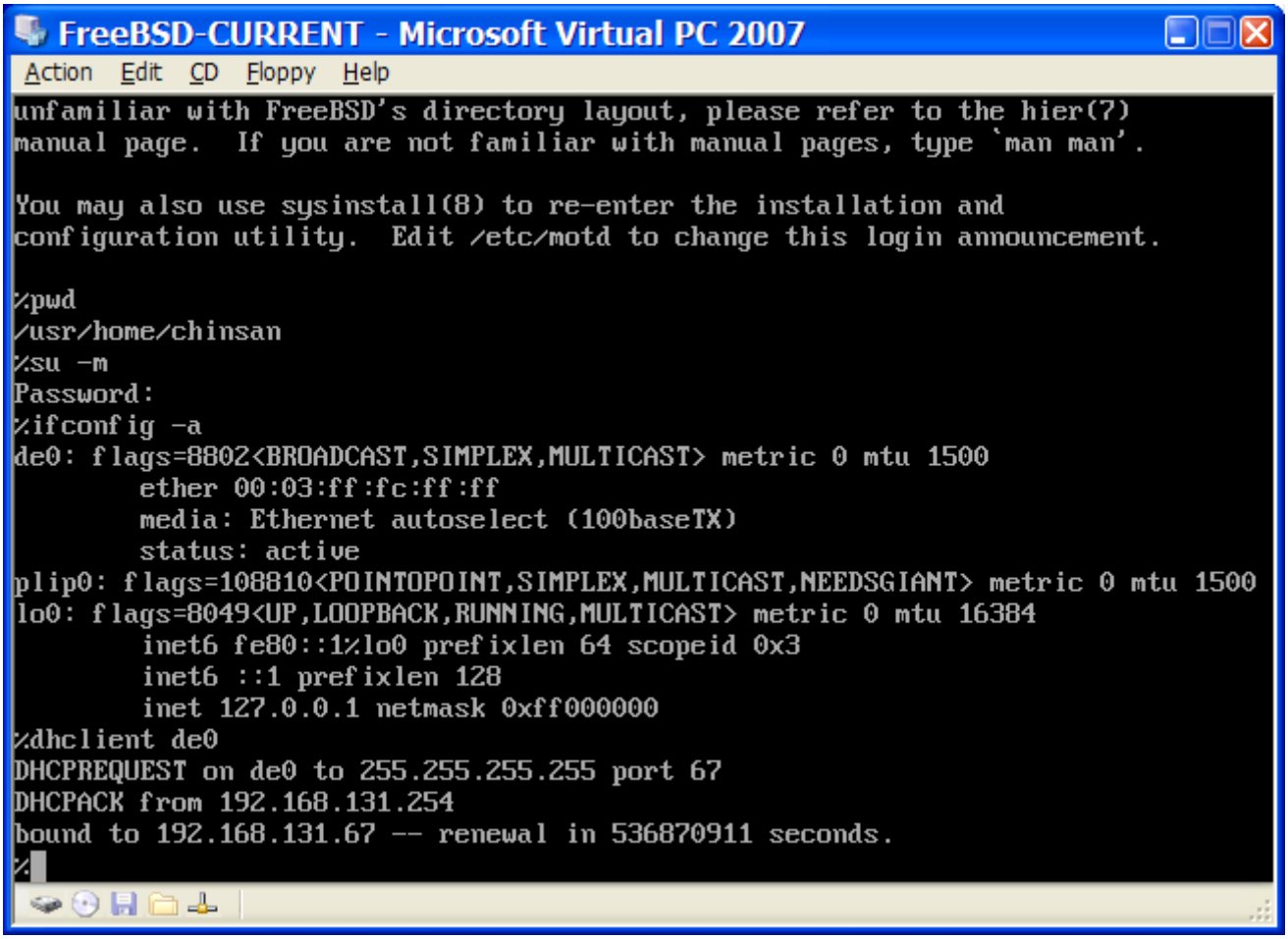
Μόλις δημιουργήσετε τη συσχέτιση με την πηγή που θα χρησιμοποιήσετε ως CDROM, επανεκκινήστε το εικονικό σας FreeBSD μηχάνημα, επιλέγοντας **Reset** από το μενού **Action**. Το Virtual PC εκκινεί με ένα ειδικό BIOS το οποίο ελέγχει πρώτα αν υπάρχει CDROM στον οδηγό, όπως ακριβώς συμβαίνει και με ένα φυσιολογικό BIOS.



Στη δική μας περίπτωση, θα ανιχνεύσει το μέσο εγκατάστασης του FreeBSD και θα ξεκινήσει η συνηθισμένη διαδικασία εγκατάστασης μέσω του sysinstall, όπως περιγράφεται στο Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων. Μπορείτε να προχωρήσετε με την εγκατάσταση, αλλά μη προσπαθήσετε να ρυθμίσετε το γραφικό σύστημα X11 τη δεδομένη στιγμή.



Όταν τελειώσετε την εγκατάσταση, μη ξεχάσετε να βγάλετε το CDROM από τον οδηγό (ή να καταργήσετε την αντίστοιχη συσχέτιση με το αρχείο ISO). Μπορείτε έπειτα να επανεκκινήσετε στη νέα σας εγκατάσταση του FreeBSD.



42.2.2.2. Ρύθμιση του FreeBSD στο Virtual PC σε Microsoft® Windows®

Μετά την επιτυχή εγκατάσταση του FreeBSD στα Microsoft® Windows® μέσω του Virtual PC, θα πρέπει να εκτελέσετε μια σειρά από ρυθμίσεις για να βελτιστοποιήσετε την λειτουργία του συστήματος σε περιβάλλον εικονικής μηχανής.

1. Θέστε Τιμές στις Μεταβλητές του Φορτωτή Εκκίνησης

   Η πιο σημαντική ρύθμιση είναι να μειώσετε την τιμή της μεταβλητής `kern.hz` για να μειώσετε τη χρήση της CPU στο FreeBSD όταν το χρησιμοποιείτε στο εικονικό περιβάλλον του Virtual PC. Αυτό μπορεί να επιτευχθεί προσθέτοντας την παρακάτω γραμμή στο αρχείο /boot/loader.conf:

   ```
   kern.hz=100
   ```

   Χωρίς αυτή τη ρύθμιση, μια εικονική μηχανή FreeBSD στο Virtual PC, όταν εκτελείται χωρίς φορτίο, θα χρησιμοποιεί περίπου το 40% του επεξεργαστή σε ένα μηχάνημα με μία CPU. Μετά από την αλλαγή αυτή, η χρήση θα είναι κοντά στο 3%.

2. Δημιουργήστε Ένα Νέο Αρχείο Ρυθμίσεων Πυρήνα

   Μπορείτε να αφαιρέσετε όλα τα προγράμματα οδήγησης για συσκευές SCSI, Firewire και USB. Το Virtual PC παρέχει μια εικονική κάρτα δικτύου η οποία υποστηρίζεται από το πρόγραμμα οδήγησης de(4), άρα μπορείτε να αφαιρέσετε όλες τις άλλες κάρτες δικτύου από τον πυρήνα, εκτός από το de(4) και το miibus(4).

3. Ρύθμιση Δικτύου

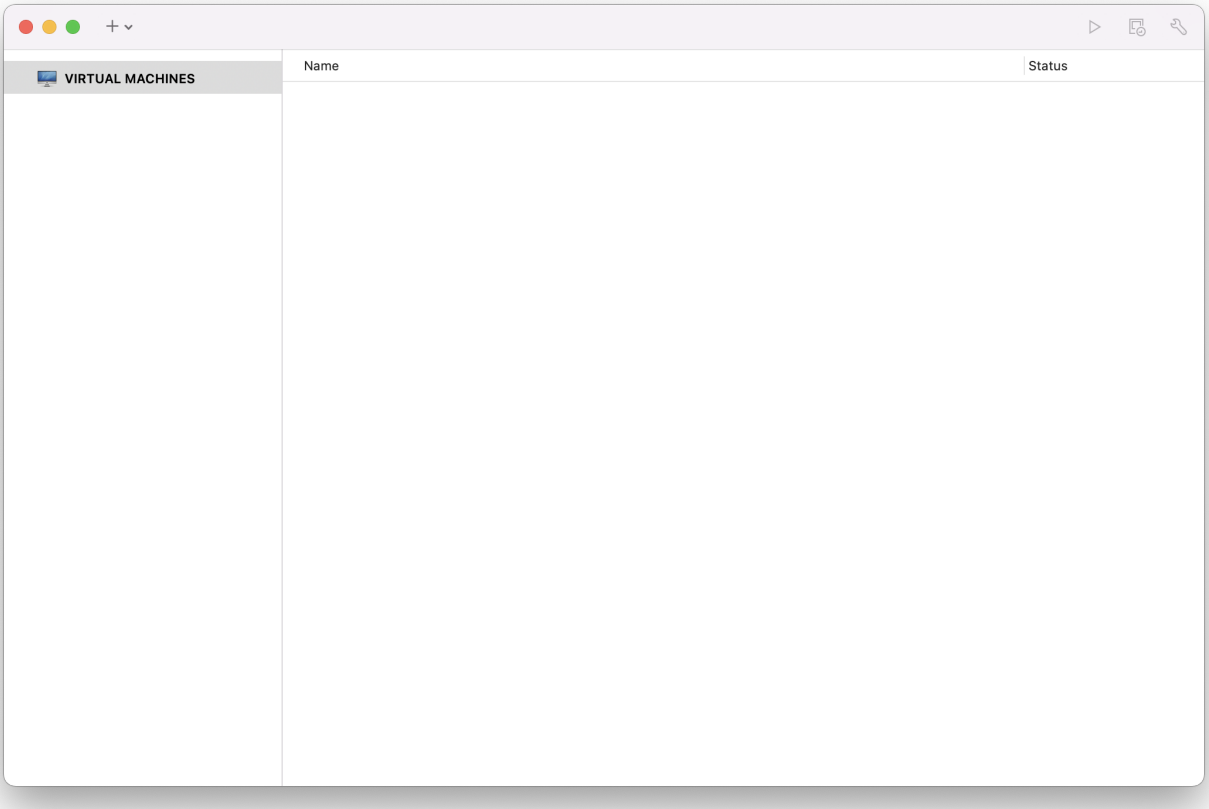
   Η πιο απλή ρύθμιση δικτύου περιλαμβάνει τη χρήση του πρωτοκόλλου DHCP για να συνδέσετε το εικονικό μηχάνημα σας στο ίδιο τοπικό δίκτυο με το μηχάνημα ξενιστή. Αυτό επιτυγχάνεται προσθέτοντας τη γραμμή `ifconfig_de0="DHCP"` στο /etc/rc.conf. Μπορείτε να βρείτε πιο προχωρημένες ρυθμίσεις δικτύου στο Προχωρημένα Θέματα Δικτύωσης.

42.2.3. Το VMware σε MacOS

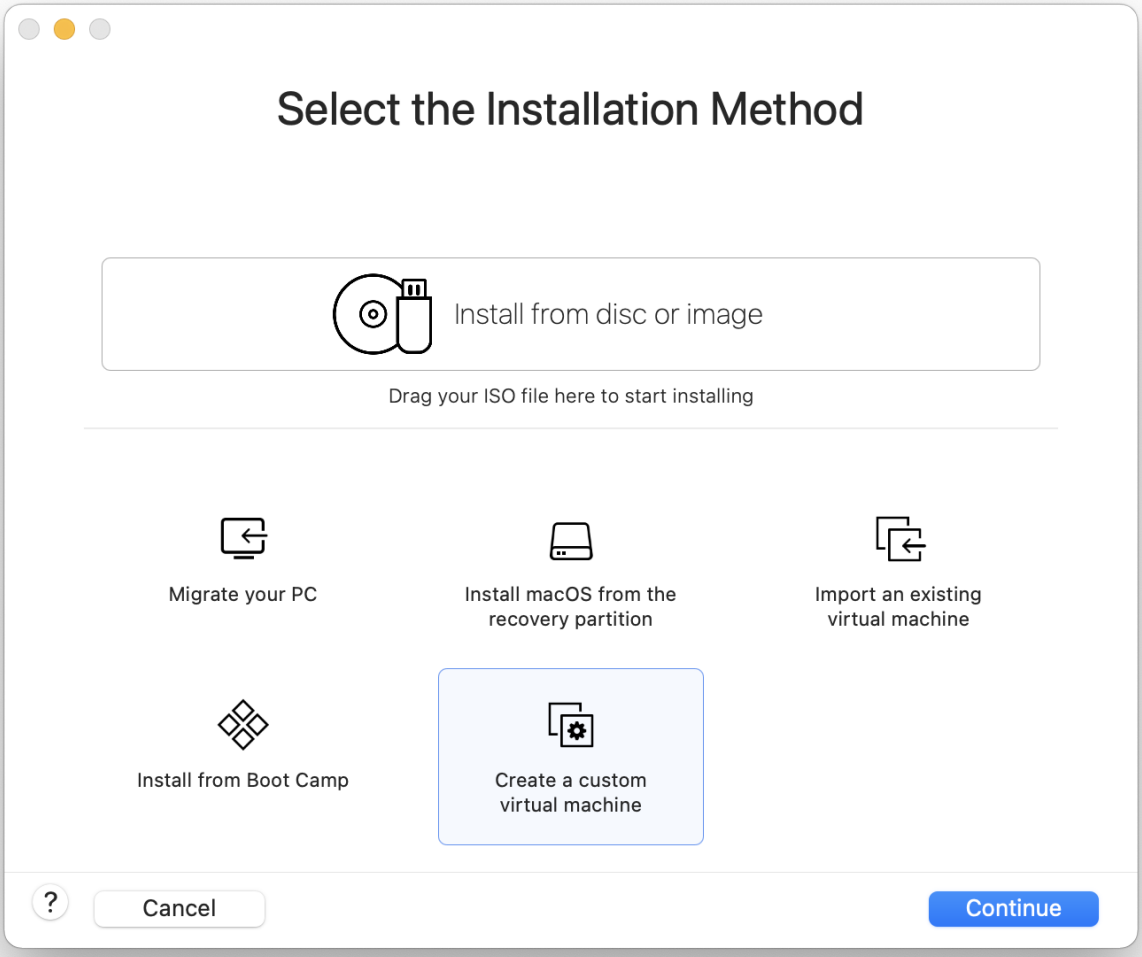
Το VMware Fusion για Mac® είναι ένα εμπορικό πρόγραμμα. Υπάρχει διαθέσιμο για υπολογιστές Apple® Mac® αρχιτεκτονικής Intel® που τρέχουν Mac OS® 10.4.9 ή κάποια πιο πρόσφατη έκδοση. Το FreeBSD υποστηρίζεται πλήρως ως φιλοξενούμενο (guest) λειτουργικό. Μόλις ολοκληρωθεί η εγκατάσταση του VMware Fusion στο Mac OS® X, πρέπει να ρυθμίσετε μια εικονική μηχανή και να εγκαταστήσετε το φιλοξενούμενο λειτουργικό σύστημα.

42.2.3.1. Εγκατάσταση του FreeBSD στο VMware/Mac OS® X

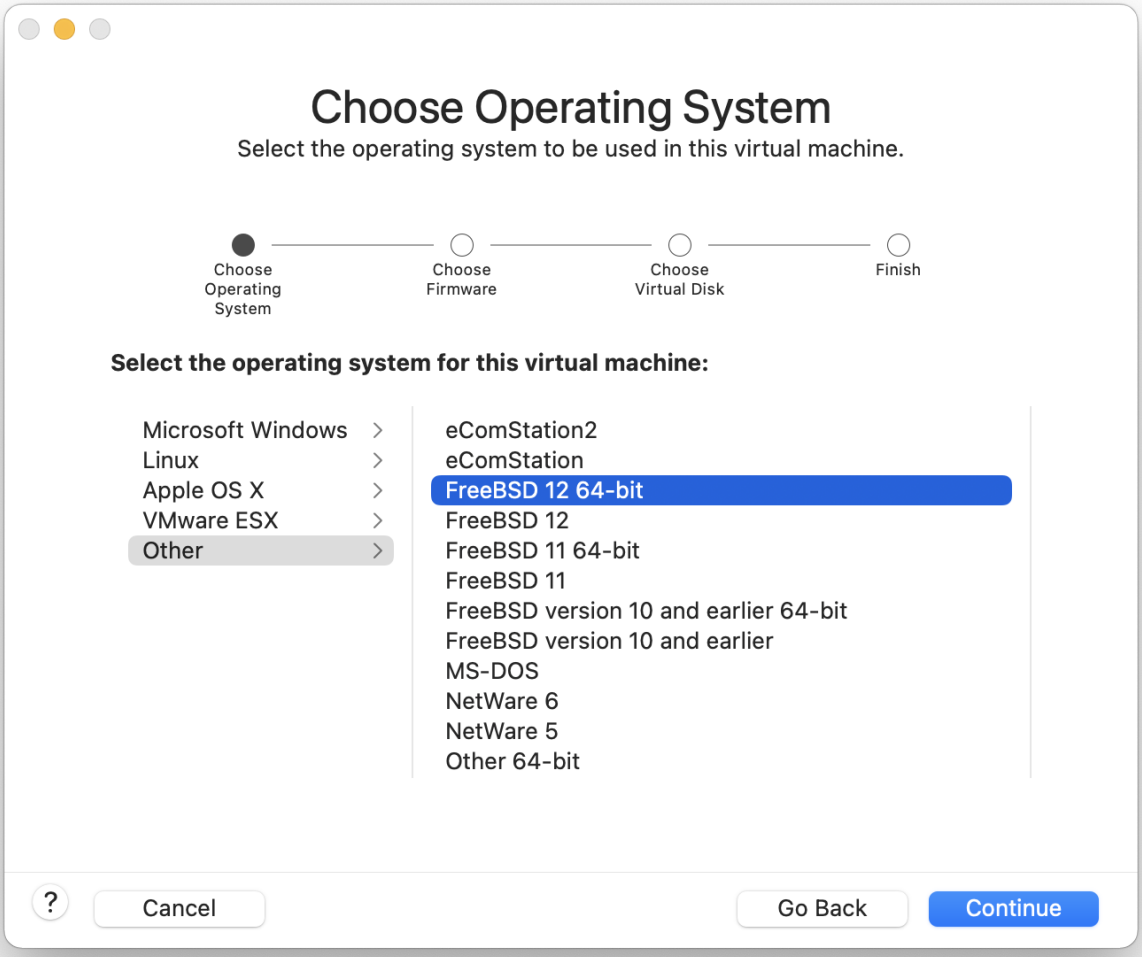
Αρχικά ξεκινήστε το VMware Fusion, και θα φορτώσει η Συλλογή Εικονικών Μηχανών. Επιλέξτε "New" για να δημιουργήσετε μια νέα εικονική μηχανή:



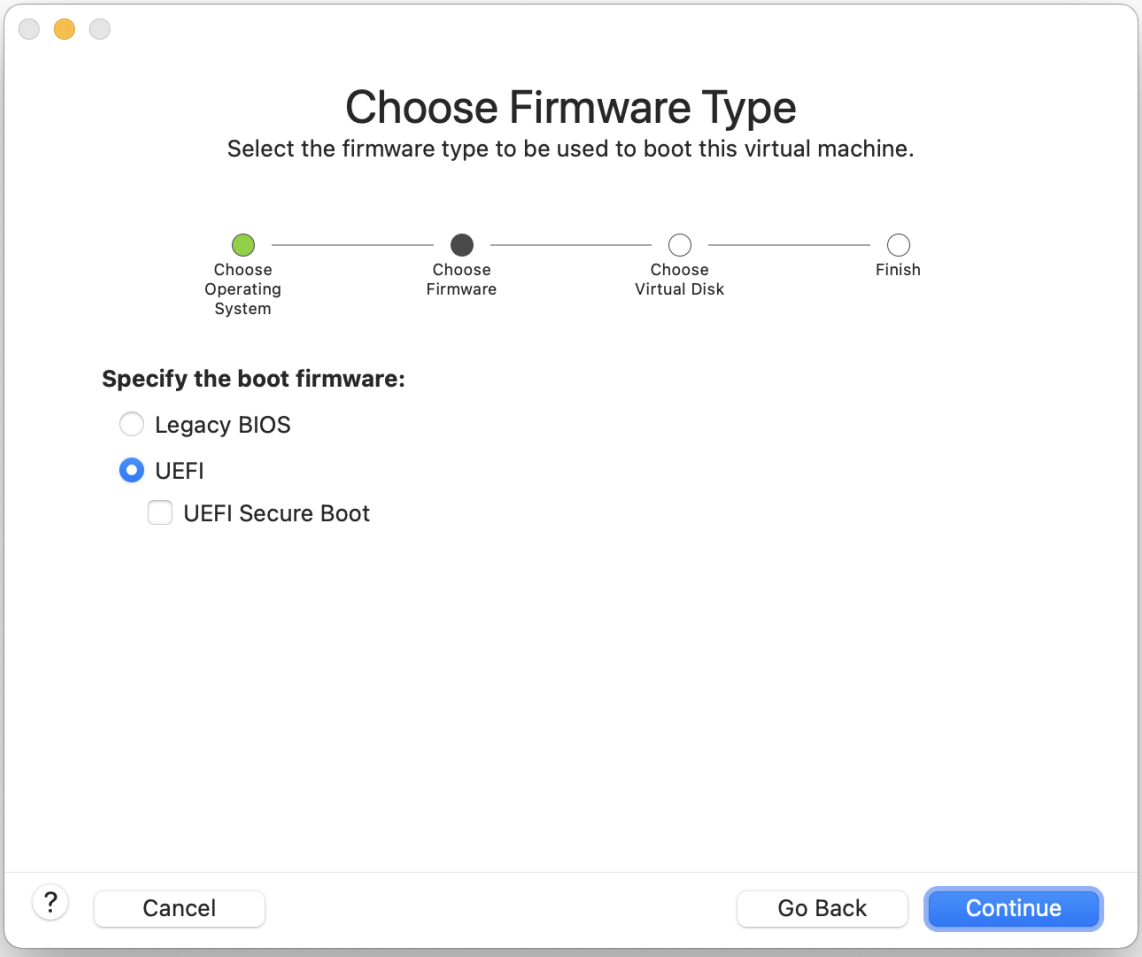
Θα δείτε να φορτώνει το New Virtual Machine Assistant, το βοηθητικό πρόγραμμα δημιουργίας μιας νέας εικονικής μηχανής. Επιλέξτε Continue για να συνεχίσετε:



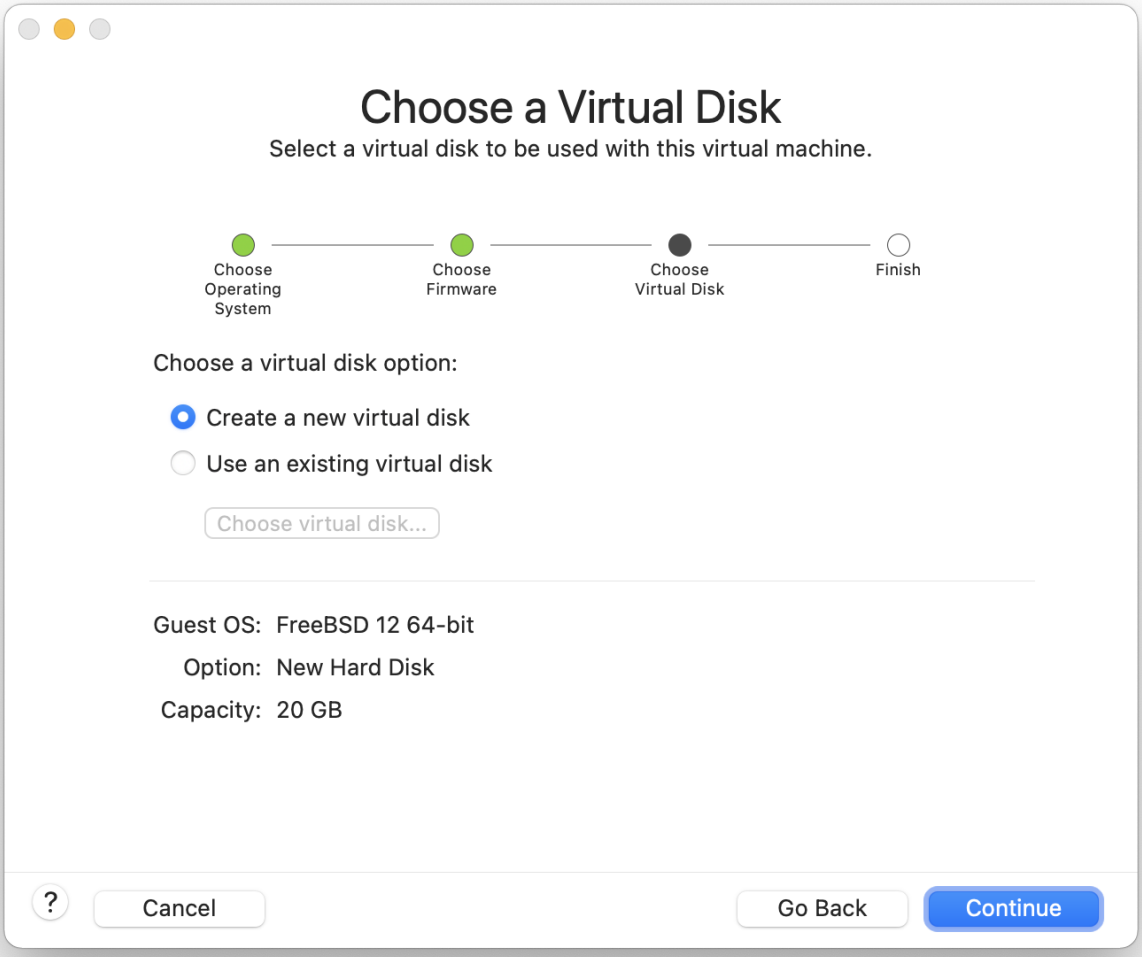
Στην επιλογή λειτουργικού συστήματος διαλέξτε Other και ως έκδοση λειτουργικού συστήματος διαλέξτε FreeBSD ή FreeBSD 64-bit (ανάλογα με το αν θέλετε υποστήριξη για 64-bit εφαρμογές ή όχι):



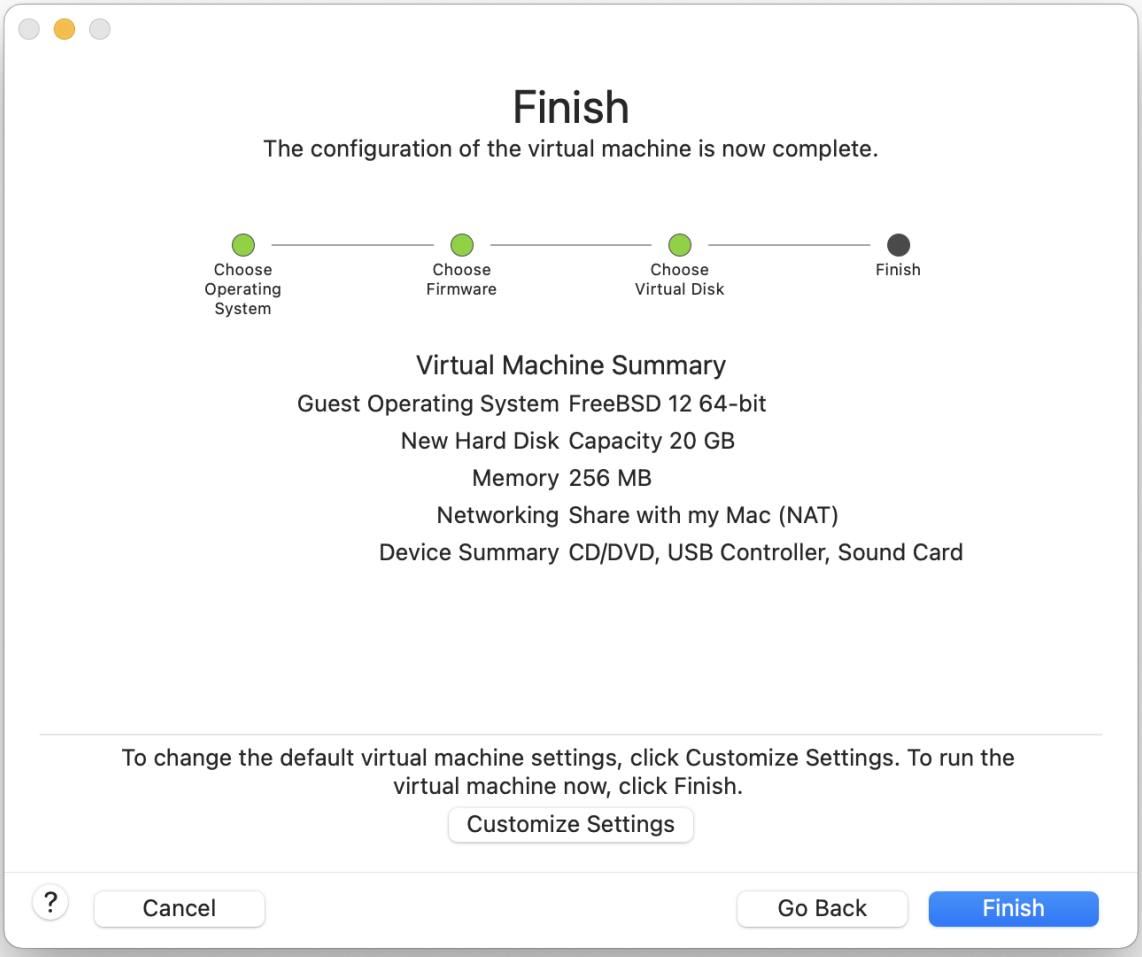
Δώστε ένα όνομα για το VM Image και ρυθμίστε τον κατάλογο στον οποίο θέλετε να αποθηκευθεί:



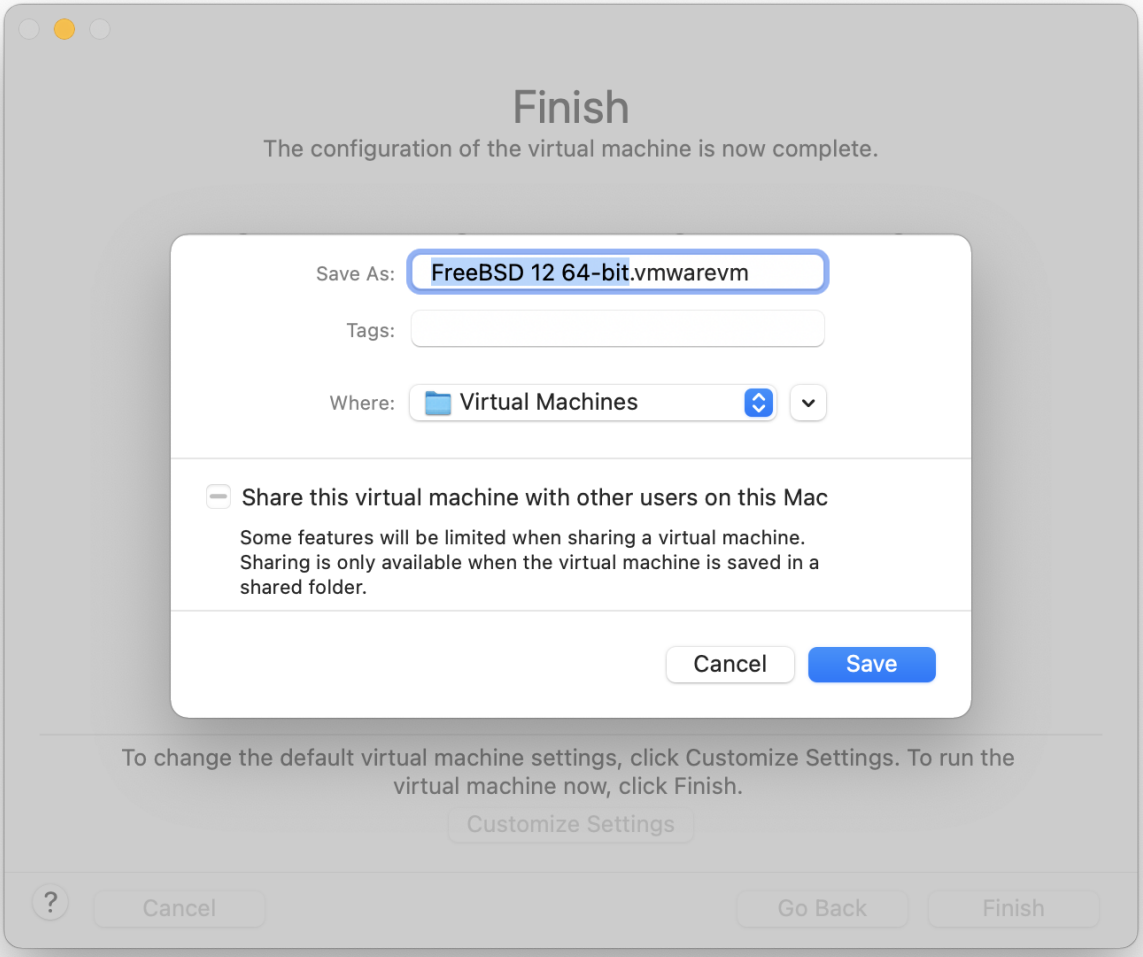
Ρυθμίστε το μέγεθος του Εικονικού Δίσκου για την εικονική μηχανή:



Επιλέξτε μια μέθοδο εγκατάστασης για την εικονική μηχανή: είτε από ένα ISO image είτε από το CD-ROM:



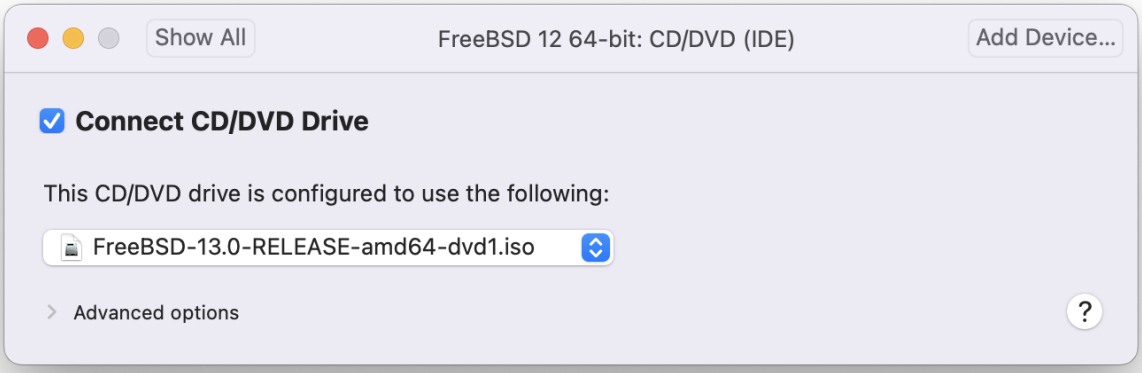
Μόλις επιλέξετε Finish, η εικονική μηχανή θα ξεκινήσει τη διαδικασία εκκίνησης (boot):



Εγκαταστήστε το FreeBSD όπως θα κάνατε και σε οποιοδήποτε άλλο υπολογιστή, ή ακολουθώντας τις οδηγίες από το Εγκατάσταση του FreeBSD 8.x και Προγενέστερων Εκδόσεων:

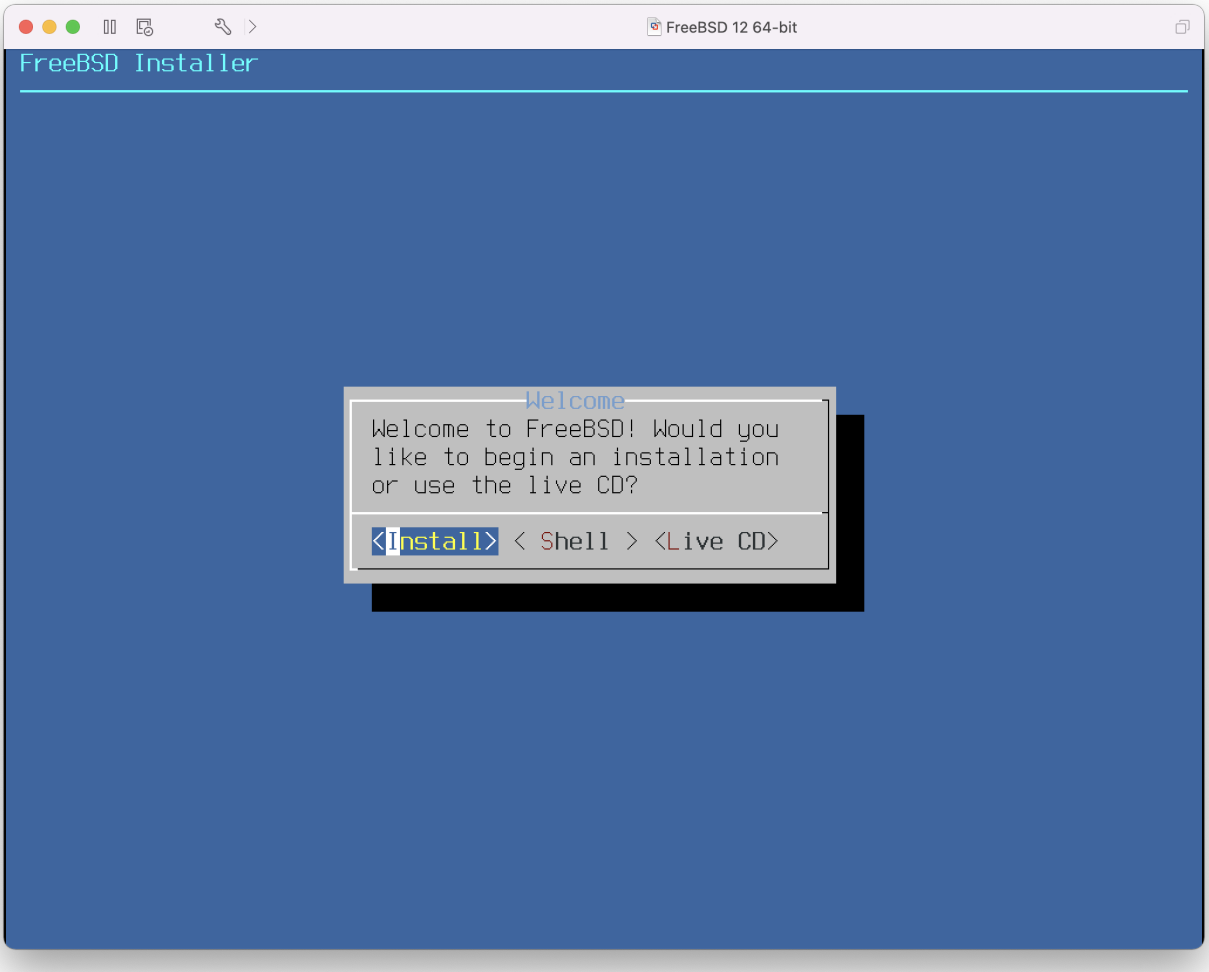
Μόλις ολοκληρωθεί η εγκατάσταση, μπορείτε να αλλάξετε τις ρυθμίσεις της εικονικής μηχανής, όπως π.χ. το μέγεθος μνήμης που θα χρησιμοποιεί:

Οι ρυθμίσεις υλικού μιας εικονικής μηχανής δε μπορούν να αλλάξουν όσο τρέχει αυτή η εικονική μηχανή.

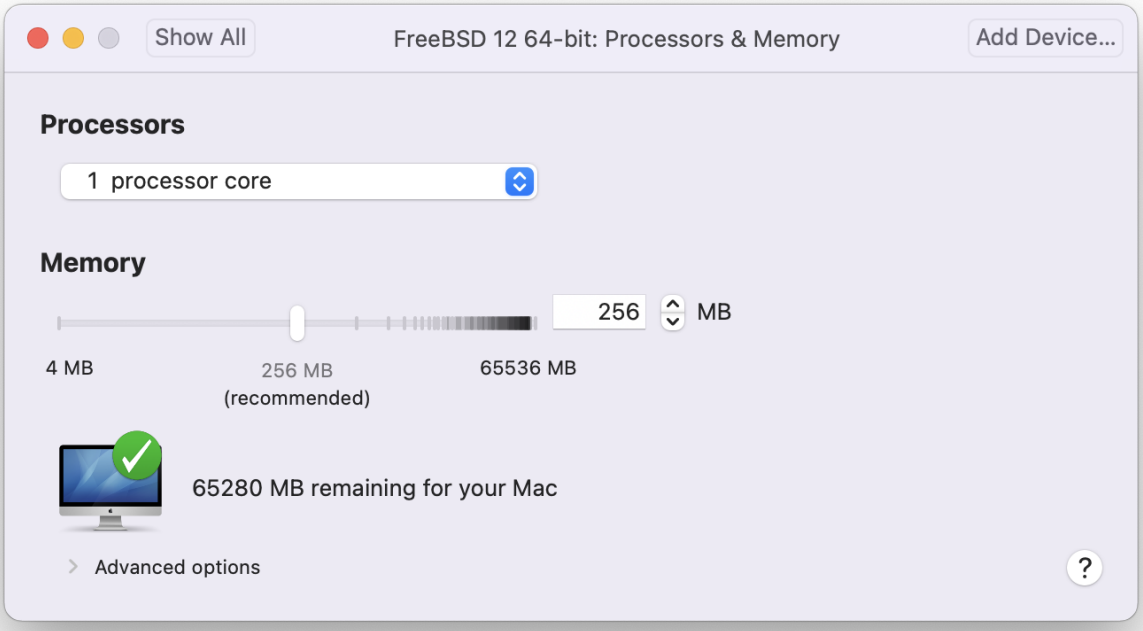


Μπορείτε, ακόμη, να ρυθμίσετε τον αριθμό των επεξεργαστών τους οποίους επιτρέπεται να χρησιμοποιήσει αυτή η εικονική μηχανή:

Ίσως έχει νόημα, επίσης, να αλλάξετε το αρχείο ή τη συσκευή που φαίνεται ως CD-ROM μέσα στην εικονική μηχανή. Συνήθως μπορείτε να αποσυνδέσετε το CD-ROM ή το ISO image από την εικονική μηχανή, αφού δε χρειάζεται πλέον όταν έχει ολοκληρωθεί η εγκατάσταση του FreeBSD:



Μια από τις τελευταίες ρυθμίσεις είναι η σύνδεση της εικονικής μηχανής με το δίκτυο. Για να μπορείτε να συνδεθείτε στην EM από άλλα μηχανήματα (εκτός του ξενιστή), ενεργοποιήστε την επιλογή Connect directly to the physical network (Bridged). Αλλιώς, για να μπορεί η EM να συνδεθεί στο δίκτυο μέσω του ξενιστή, αλλά να μη μπορούν άλλα μηχανήματα να συνδεθούν σε αυτή, ενεργοποιήστε την επιλογή Share the host's internet connection (NAT).



Μόλις τελειώσετε με αυτές τις ρυθμίσεις, μπορείτε να εκκινήσετε τη νέα εικονική μηχανή με το φρεσκο-εγκατεστημένο FreeBSD σας.

42.2.3.2. Ρυθμίσεις του FreeBSD μέσα στο Mac OS® X/VMware

Αφού τελειώσετε με την εγκατάσταση του FreeBSD σε μια εικονική μηχανή VMware μέσα σε Mac OS® X, πρέπει να κάνετε κάποιες ρυθμίσεις για να βελτιωθεί η απόδοση του FreeBSD ως φιλοξενούμενου συστήματος.

1. Ρυθμίσεις Μεταβλητών του Boot Loader

   Η πιο σημαντική ρύθμιση είναι να μειώσετε την τιμή της μεταβλητής `kern.hz`, για να μειωθεί κάπως η χρήση του επεξεργαστή από το FreeBSD καθώς τρέχει μέσα στο VMware. Προσθέστε, λοιπόν, την παρακάτω γραμμή στο αρχείο /boot/loader.conf:

   ```
   kern.hz=100
   ```

   Χωρίς αυτή τη ρύθμιση ένα φιλοξενούμενο FreeBSD που τρέχει μέσα σε VMware μπορεί να χρησιμοποιεί μέχρι και 15% του επεξεργαστή ενός iMac®. Μετά από αυτή τη ρύθμιση η χρήση του επεξεργαστή μπορεί να είναι μικρότερη από 5%.

2. Δημιουργήστε Ένα Νέο Αρχείο Ρυθμίσεων Πυρήνα

   Μπορείτε να αφαιρέσετε όλες τις συσκευές FireWire και USB. Το VMware παρέχει μια εικονική κάρτα δικτύου, η οποία είναι συμβατή με τον οδηγό em(4), οπότε μπορείτε να αφαιρέσετε όλες τις υπόλοιπες κάρτες δικτύου από τον πυρήνα σας.

3. Ρυθμίστε το Δίκτυο

Ο πιο εύκολος τρόπος να ρυθμίσετε το δίκτυο της εικονικής μηχανής είναι να συνδεθείτε μέσω DHCP με το τοπικό δίκτυο, χρησιμοποιώντας τη διεύθυνση MAC του ξενιστή. Αυτό μπορεί να γίνει προσθέτοντας τη γραμμή `ifconfig_em0="DHCP"` στο αρχείο /etc/rc.conf. Για περισσότερες πληροφορίες και πιο προχωρημένες ρυθμίσεις δικτύου, δείτε το Προχωρημένα Θέματα Δικτύωσης.

42.2.4. VirtualBox™ Guest Additions σε FreeBSD Guest

Τα πρόσθετα προγράμματα για το φιλοξενούμενο λειτουργικό (guest additions) του VirtualBox™ παρέχουν υποστήριξη για τα παρακάτω:

- Κοινή χρήση προχείρου (clipboard)
- Έξυπνη χρήση δείκτη ποντικιού
- Συγχρονισμός ώρας με τον ξενιστή (host)
- Αναπροσαρμογή μεγέθους παραθύρου
- Κατάσταση απρόσκοπτης λειτουργίας (seamless mode)

Οι παρακάτω εντολές εκτελούνται στο φιλοξενούμενο FreeBSD λειτουργικό.

Αρχικά, εγκαταστήστε το πακέτο emulators/virtualbox-ose-additions στο φιλοξενούμενο FreeBSD λειτουργικό.

```
# cd /usr/ports/emulators/virtualbox-ose-additions && make install clean
```

Προσθέστε τις παρακάτω γραμμές στο /etc/rc.conf:

```
vboxguest_enable="YES"
vboxservice_enable="YES"
```

Αν πρόκειται να χρησιμοποιήσετε το ntpd(8) ή το ntpdate(8), θα πρέπει να απενεργοποιήσετε το συγχρονισμό ώρας με τον ξενιστή:

```
vboxservice_flags="--disable-timesync"
```

Το πρόγραμμα οδήγησης `vboxvideo_drv` φυσιολογικά θα αναγνωριστεί αυτόματα όταν εκτελέσετε το `Xorg -configure`. Αν αυτό δεν συμβεί, τροποποιήστε το xorg.conf για την κάρτα γραφικών του VirtualBox™:

```
Section "Device"
    ### Available Driver options are:-
    ### Values: <i>: integer, <f>: float, <bool>: "True"/"False",
    ### <string>: "String", <freq>: "<f> Hz/kHz/MHz"
    ### [arg]: arg optional
    Identifier "Card0"
```

```
    Driver "vboxvideo"
    VendorName "InnoTek Systemberatung GmbH"
    BoardName "VirtualBox Graphics Adapter"
    BusID "PCI:0:2:0"
EndSection
```

Για να χρησιμοποιήσετε το vboxmouse_drv, χρησιμοποιήστε την παρακάτω ενότητα για το ποντίκι στο xorg.conf:

```
Section "InputDevice"
    Identifier "Mouse0"
    Driver "vboxmouse"
EndSection
```

Οι χρήστες του HAL θα πρέπει να δημιουργήσουν το αρχείο /usr/local/etc/hal/fdi/policy/90-vboxguest.fdi ή να το αντιγράψουν από το /usr/local/shared/hal/fdi/policy/10osvendor/90-vboxguest.fdi:

```
<?xml version="1.0" encoding="utf-8"?>
<!--
# Sun VirtualBox
# Hal driver description for the vboxmouse driver
# $Id: chapter.xml,v 1.16 2011-12-09 19:53:53 manolis Exp $

    Copyright (C) 2008-2009 Sun Microsystems, Inc.

    This file is part of VirtualBox Open Source Edition (OSE, as
    available from http://www.virtualbox.org. This file is free software;
    you can redistribute it and/or modify it under the terms of the GNU
    General Public License (GPL) as published by the Free Software
    Foundation, in version 2 as it comes in the "COPYING" file of the
    VirtualBox OSE distribution. VirtualBox OSE is distributed in the
    hope that it will be useful, but WITHOUT ANY WARRANTY of any kind.

    Please contact Sun Microsystems, Inc., 4150 Network Circle, Santa
    Clara, CA 95054 USA or visit http://www.sun.com if you need
    additional information or have any questions.
-->
<deviceinfo version="0.2">
  <device>
    <match key="info.subsystem" string="pci">
      <match key="info.product" string="VirtualBox guest Service">
        <append key="info.capabilities" type="strlist">input</append>
    <append key="info.capabilities" type="strlist">input.mouse</append>
        <merge key="input.x11_driver" type="string">vboxmouse</merge>
    <merge key="input.device" type="string">/dev/vboxguest</merge>
      </match>
    </match>
```

```
  </device>
</deviceinfo>
```

42.3. Το FreeBSD ως Ξενιστής (Host)

Για αρκετά χρόνια, κανένα από τα πακέτα εικονικοποίησης δεν υποστήριζε επίσημα το FreeBSD ως ξενιστή. Κάποιοι χρήστες χρησιμοποιούσαν παλιές και κατά βάση εγκαταλελειμμένες εκδόσεις του VMware (όπως το emulators/vmware3), οι οποίες χρησιμοποιούσαν την συμβατότητα εκτέλεσης προγραμμάτων Linux®. Λίγο μετά την επίσημη κυκλοφορία του FreeBSD 7.2, έγινε διαθέσιμη στη Συλλογή των Ports η εφαρμογή VirtualBox™ της Sun™. Η εφαρμογή αυτή εκτελείται ως εγγενές πρόγραμμα του FreeBSD.

Το VirtualBox™ είναι ένα πλήρες πακέτο εικονικοποίησης το οποίο βρίσκεται σε διαρκή ανάπτυξη. Είναι διαθέσιμο για τα περισσότερα λειτουργικά συστήματα, συμπεριλαμβανομένων των Windows®, Mac OS®, Linux® και FreeBSD. Έχει τη δυνατότητα να εκτελεί το ίδιο καλά τόσο λειτουργικά τύπου Windows® όσο και UNIX®. Διανέμεται ως λογισμικό ανοικτού κώδικα αλλά περιέχει κάποια εξαρτήματα κλειστού κώδικα που διατίθενται ως χωριστό πακέτο επέκτασης. Μπορείτε να βρείτε περισσότερες πληροφορίες στη σελίδα "Downloads" στο wiki του VirtualBox™, http://www.virtualbox.org/wiki/Downloads. Τη δεδομένη στιγμή οι επεκτάσεις αυτές δεν διατίθενται για το FreeBSD.

42.3.1. Εγκατάσταση του VirtualBox™

Το VirtualBox™ είναι διαθέσιμο ως FreeBSD port στο emulators/virtualbox-ose. Καθώς το VirtualBox™ βρίσκεται υπό συνεχή και πολύ ενεργή ανάπτυξη, βεβαιωθείτε ότι έχετε ανανεώσει το δέντρο των ports πριν ξεκινήσετε την εγκατάσταση του. Χρησιμοποιήστε τις παρακάτω εντολές για να το εγκαταστήσετε:

```
# cd /usr/ports/emulators/virtualbox-ose
# make install clean
```

Μια χρήσιμη επιλογή που εμφανίζεται στο διάλογο ρυθμίσεων, αφορά την εγκατάσταση των προγραμμάτων `GuestAdditions`. Τα προγράμματα αυτά παρέχουν μια σειρά από χρήσιμες λειτουργίες στα φιλοξενούμενα λειτουργικά, όπως η διάφανη λειτουργία του δείκτη ποντικιού (επιτρέπει στο ποντίκι να κινείται ελεύθερα μεταξύ του ξενιστή και του φιλοξενούμενου λειτουργικού, χωρίς να απαιτείται η χρήση κάποιου ειδικού πλήκτρου για εναλλαγή) καθώς και ταχύτερη γραφική απεικόνιση, ειδικά σε λειτουργικά Windows®. Μπορείτε να βρείτε τα guest additions στο μενού **Devices**, όταν ολοκληρώσετε την εγκατάσταση του φιλοξενούμενου λειτουργικού.

Πριν χρησιμοποιήσετε το VirtualBox™ για πρώτη φορά, θα πρέπει να αλλάξετε κάποιες ρυθμίσεις. Το port εγκαθιστά ένα άρθρωμα πυρήνα στον κατάλογο /boot/modules το οποίο θα πρέπει να φορτώσετε στον πυρήνα που εκτελείται:

```
# kldload vboxdrv
```

Για να φορτώνεται το άρθρωμα αυτόματα σε κάθε επανεκκίνηση του συστήματος, προσθέστε την παρακάτω γραμμή στο αρχείο /boot/loader.conf:

```
vboxdrv_load="YES"
```

Για να χρησιμοποιήσετε τα αρθρώματα πυρήνα που επιτρέπουν τη λειτουργία του δικτύου σε κατάσταση γέφυρας (bridged) ή host-only, προσθέστε την παρακάτω γραμμή στο /etc/rc.conf και επανεκκινήστε τον υπολογιστή σας:

```
vboxnet_enable="YES"
```

Κατά τη διάρκεια της εγκατάστασης του VirtualBox™, δημιουργείται αυτόματα η ομάδα χρηστών `vboxusers`. Όλοι οι χρήστες που χρειάζονται πρόσβαση στο VirtualBox™, θα πρέπει να ανήκουν σε αυτή την ομάδα. Μπορείτε να χρησιμοποιήσετε την εντολή `pw` για να προσθέσετε νέα μέλη στην ομάδα:

```
# pw groupmod vboxusers -m yourusername
```

Τα προεπιλεγμένα δικαιώματα για τη συσκευή /dev/vboxnetctl είναι αρκετά περιοριστικά και πρέπει να αλλάξουν για να λειτουργήσει το δίκτυο σε κατάσταση γέφυρας.

Για να δοκιμάσετε τις νέες ρυθμίσεις προσωρινά:

```
# chown root:vboxusers /dev/vboxnetctl
# chmod 0660 /dev/vboxnetctl
```

Για να αλλάξετε τα δικαιώματα μόνιμα, προσθέστε τις παρακάτω γραμμές στο /etc/devfs.conf:

```
own     vboxnetctl root:vboxusers
perm    vboxnetctl 0660
```

Για να εκτελέσετε το VirtualBox™, μπορείτε απλώς να επιλέξετε την καταχώριση Sun VirtualBox από το μενού του γραφικού σας περιβάλλοντος, ή να πληκτρολογήσετε το παρακάτω σε ένα τερματικό:

```
% VirtualBox
```

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση και χρήση του VirtualBox™, παρακαλούμε επισκεφθείτε την επίσημη δικτυακή τοποθεσία στο http://www.virtualbox.org. Καθώς το FreeBSD port είναι πολύ πρόσφατο, η εξέλιξη του είναι συνεχής. Για τις τελευταίες πληροφορίες καθώς και για οδηγίες αντιμετώπισης τυχόν προβλημάτων, παρακαλούμε δείτε τη σχετική σελίδα στο wiki του FreeBSD, στην τοποθεσία http://wiki.FreeBSD.org/VirtualBox.

42.3.2. Υποστήριξη USB στο VirtualBox™

Για τα βήματα αυτά απαιτείται το VirtualBox™ 4.0.0 ή μεταγενέστερο.

Για να μπορείτε να διαβάσετε και να γράψετε σε συσκευές USB, θα πρέπει ο λογαριασμός σας να ανήκει στην ομάδα operators:

```
# pw groupmod operator -m jerry
```

Προσθέστε έπειτα τις παρακάτω γραμμές στο αρχείο /etc/devfs.rules (δημιουργήστε το αν δεν υπάρχει ήδη):

```
[system=10]
add path 'usb/*' mode 0660 group operator
```

Για να φορτώσετε τους νέους κανόνες, προσθέστε την παρακάτω γραμμή στο /etc/rc.conf:

```
devfs_system_ruleset="system"
```

Έπειτα επανεκκινήστε το devfs:

```
# /etc/rc.d/devfs restart
```

Μπορείτε τώρα να ενεργοποιήσετε το USB στο φιλοξενούμενο λειτουργικό. Θα πρέπει να μπορείτε να δείτε τις συσκευές USB στις προτιμήσεις του VirtualBox™.

42.3.3. Πρόσβαση στο DVD/CD του Ξενιστή

θα πρέπει να φορτώσετε το άρθρωμα πυρήνα `atapicam` προσθέτοντας την παρακάτω γραμμή στο /boot/loader.conf:

```
atapicam_load="YES"
```

Θα πρέπει να εκτελείται το HAL για να λειτουργήσει σωστά το DVD/CD στο VirtualBox™. Ενεργοποιήστε το στο /etc/rc.conf και ξεκινήστε το (αν δεν εκτελείται ήδη):

```
hald_enable="YES"
```

```
# /usr/local/etc/rc.d/hald start
```

Για να μπορούν οι χρήστες να έχουν πρόσβαση στις λειτουργίες CD/DVD του VirtualBox™, χρειάζονται πρόσβαση στις συσκευές /dev/xpt0, /dev/cdN και /dev/passN. Προσθέστε τις παρακάτω

γραμμές στο /etc/devfs.conf:

```
perm cd0 0600
perm xpt0 0660
perm pass0 0660
```

Chapter 43. Τοπικές Ρυθμίσεις - Χρήση και ρύθμιση I18N/L10N

43.1. Σύνοψη

Το FreeBSD είναι ένα ιδιαίτερα αποκεντρωμένο έργο με χρήστες και εθελοντές σε ολόκληρο τον κόσμο. Στο κεφάλαιο αυτό συζητούνται οι δυνατότητες τοπικών και διεθνών ρυθμίσεων του FreeBSD, οι οποίες επιτρέπουν σε χρήστες γλωσσών εκτός της Αγγλικής να εκτελέσουν πραγματική εργασία. Υπάρχουν πολλοί παράγοντες στην υλοποίηση του πλαισίου i18n, τόσο σε επίπεδο συστήματος, όσο και εφαρμογών, και για το λόγο αυτό, όπου χρειάζεται, παραπέμπουμε τον αναγνώστη σε πιο συγκεκριμένες πηγές τεκμηρίωσης.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως κωδικοποιούνται οι γλώσσες και οι τοπικές ρυθμίσεις στα σύγχρονα λειτουργικά συστήματα.
- Πως να βάλετε τοπικές ρυθμίσεις στο κέλυφος σας (login shell).
- Πως να ρυθμίσετε την κονσόλα για γλώσσες εκτός της Αγγλικής.
- Πως να χρησιμοποιήσετε αποτελεσματικά το σύστημα X Windows με διαφορετικές γλώσσες.
- Που να βρείτε περισσότερες πληροφορίες για τη συγγραφή εφαρμογών συμβατών με το πρότυπο i18n.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

43.2. Βασικές Γνώσεις

43.2.1. Τι Είναι το I18N/L10N;

Οι ομάδες ανάπτυξης λογισμικού δημιούργησαν τον όρο I18N, ως συντόμευση της λέξης "internationalization" (διεθνοποίηση), μετρώντας απλώς τα γράμματα της λέξης ανάμεσα στο πρώτο και το τελευταίο. Ο όρος L10N έχει προκύψει με τον ίδιο τρόπο, αυτή τη φορά από τη λέξη "localization" (τοπικοποίηση, ή απλώς τοπικές ρυθμίσεις). Συνδυάζοντας μεταξύ τους τις μεθόδους, τα πρωτόκολλα, και τις εφαρμογές που συμβαδίζουν με τα I18N/L10N, οι χρήστες μπορούν να χρησιμοποιήσουν τις γλώσσες της επιλογής τους.

Οι εφαρμογές I18N προγραμματίζονται με τη βοήθεια εργαλείων (kits) και βιβλιοθηκών. Επιτρέπεται έτσι στους προγραμματιστές να γράψουν ένα απλό αρχείο και να μεταφράσουν τα μενού και τα κείμενα που απεικονίζει η εφαρμογή, σε κάθε γλώσσα που απαιτείται. Συνιστούμε ένθερμα στους προγραμματιστές να ακολουθούν την παραπάνω σύμβαση.

43.2.2. Γιατί Πρέπει να Χρησιμοποιήσω τα I18N/L10N;

Τα I18N/L10N χρησιμοποιούνται κάθε φορά που επιθυμείτε να δείτε, να εισάγετε, ή να επεξεργαστείτε δεδομένα σε γλώσσες εκτός της Αγγλικής.

43.2.3. Ποιες Γλώσσες Υποστηρίζονται στο I18N;

Το I18N και το L10N δεν είναι ειδικά φτιαγμένα για το FreeBSD. Την δεδομένη στιγμή, υποστηρίζονται οι περισσότερες γνωστές γλώσσες, συμπεριλαμβανομένων των: Κινεζικών, Γερμανικών, Γιαπωνέζικων, Κορεατικών, Γαλλικών, Ρωσικών, Βιετναμέζικων, κ.α.

43.3. Χρήση των Τοπικών Ρυθμίσεων

Το I18N είναι στην πραγματικότητα μια σύμβαση, και δεν έχει δημιουργηθεί αποκλειστικά για το FreeBSD. Επιθυμούμε τη βοήθεια σας ώστε το FreeBSD να ακολουθεί αυτή τη σύμβαση.

Οι τοπικές ρυθμίσεις βασίζονται σε τρεις βασικούς όρους: Κωδικό Γλώσσας, Κωδικό Χώρας και Κωδικοποίηση. Τα ονόματα των τοπικών ρυθμίσεων προκύπτουν από τους παραπάνω όρους, με τον τρόπο που περιγράφεται παρακάτω:

```
ΚωδικόςΓλώσσας_ΚωδικόςΧώρας.Κωδικοποίηση
```

43.3.1. Κωδικοί Γλωσσών και Χωρών

Για να χρησιμοποιηθούν οι τοπικές ρυθμίσεις για μια συγκεκριμένη γλώσσα σε ένα σύστημα FreeBSD (ή σε άλλο σύστημα τύπου UNIX® που υποστηρίζει το πρότυπο I18N), ο χρήστης θα πρέπει να βρει τους κωδικούς της συγκεκριμένης χώρας και γλώσσας (οι κωδικοί χωρών καθοδηγούν τις εφαρμογές σχετικά με τη διάλεκτο της γλώσσας που πρέπει να χρησιμοποιηθεί). Προγράμματα όπως φυλλομετρητές, εξυπηρετητές ιστοσελίδων, εξυπηρετητές SMTP/POP κλπ. παίρνουν επίσης κάποιες αποφάσεις που εξαρτώνται από τους κωδικούς αυτούς. Παρακάτω φαίνονται μερικά παραδείγματα γλωσσών/χωρών:

Κωδικός Γλώσσας/Χώρας	**Περιγραφή**
en_US	Αγγλικά - Ηνωμένες Πολιτείες
ru_RU	Ρώσικα - Ρωσία
zh_TW	Παραδοσιακά Κινέζικα - Ταϊβάν

43.3.2. Κωδικοποιήσεις

Κάποιες γλώσσες χρησιμοποιούν κωδικοποιήσεις που δεν είναι ASCII, αλλά περιέχουν χαρακτήρες 8-bit, wide, ή multibyte (δείτε τη σελίδα manual multibyte(3) για περισσότερες πληροφορίες). Οι πιο καινούριες εφαρμογές συνήθως αναγνωρίζουν τους χαρακτήρες 8-bit. Ανάλογα με την υλοποίηση, οι χρήστες μπορεί να χρειάζεται να μεταγλωττίσουν μια εφαρμογή με υποστήριξη χαρακτήρων wide ή multibyte, ή να προσαρμόσουν τις ρυθμίσεις του προγράμματος. Για να έχετε την ικανότητα να εισάγετε και να επεξεργάζεστε χαρακτήρες multibyte, η Συλλογή των Ports του FreeBSD διαθέτει προγράμματα για κάθε γλώσσα. Δείτε την τεκμηρίωση για το I18N στο αντίστοιχο Port του FreeBSD.

Ειδικότερα, ο χρήστης χρειάζεται να διαβάσει την τεκμηρίωση της εφαρμογής, για να αποφασίσει πως πρέπει να τη ρυθμίσει σωστά ή πως να περάσει τις σωστές τιμές στο configure, το Makefile ή τον μεταγλωττιστή.

Θα πρέπει να έχετε κατά νου κάποια πράγματα:

- Σετ χαρακτήρων που εξαρτώνται από τη γλώσσα (single C chars character set, δείτε την multibyte(3)), π.χ. ISO8859-1, ISO8859-15, KOI8-R, CP437.
- Κωδικοποιήσεις Wide ή multibyte, π.χ. EUC, Big5.

Μπορείτε να δείτε την ενεργή λίστα των σετ χαρακτήρων στο Μητρώο IANA.

Το FreeBSD χρησιμοποιεί για τις τοπικές ρυθμίσεις κωδικοποιήσεις συμβατές με το X11.

43.3.3. Εφαρμογές I18N

Στο σύστημα πακέτων και ports του FreeBSD, οι εφαρμογές που σχετίζονται με το I18N έχουν στο όνομα τους τη λέξη `I18N` ώστε να αναγνωρίζονται εύκολα. Ωστόσο, μπορεί να μην υποστηρίζουν πάντοτε τη γλώσσα που χρειάζεστε.

43.3.4. Τοπικές Ρυθμίσεις

Είναι συνήθως αρκετό να γίνει export η τιμή με την ονομασία της επιθυμητής τοπικής ρύθμισης, μέσω της μεταβλητής περιβάλλοντος `LANG` στο κέλυφος εισόδου. Αυτό μπορεί να γίνει στο αρχείο ~/.login_conf του χρήστη, ή στο αρχείο εκκίνησης του κελύφους του χρήστη (~/.profile, ~/.bashrc, ~/.cshrc). Δεν είναι ανάγκη να θέσετε και τις υπόλοιπες μεταβλητές των τοπικών ρυθμίσεων, όπως οι `LC_CTYPE`, `LC_CTIME`. Για περισσότερες πληροφορίες, διαβάστε την τεκμηρίωση του FreeBSD που σχετίζεται με την υποστήριξη της επιθυμητής γλώσσας.

Θα πρέπει να θέσετε τις δύο παρακάτω μεταβλητές περιβάλλοντος, στα αρχεία ρυθμίσεων:

- Την `LANG` για λειτουργίες που ανήκουν στην οικογένεια POSIX® setlocale(3)
- Την `MM_CHARSET` για το σύνολο χαρακτήρων MIME των εφαρμογών.

Το παραπάνω περιλαμβάνει την ρύθμιση του κελύφους χρήστη, την ρύθμιση για μια συγκεκριμένη εφαρμογή, και τη ρύθμιση για τα X11.

43.3.4.1. Μέθοδοι Αλλαγής Τοπικών Ρυθμίσεων

Υπάρχουν δύο μέθοδοι για την αλλαγή των τοπικών ρυθμίσεων, τις οποίες και περιγράφουμε παρακάτω. Η πρώτη (την οποία και συνιστούμε) υλοποιείται θέτοντας τιμές στις μεταβλητές περιβάλλοντος στο login class, και η δεύτερη αλλάζοντας τις τιμές των μεταβλητών περιβάλλοντος στο αρχείο εκκίνησης του κελύφους του χρήστη.

43.3.4.1.1. Μέθοδος Κλάσεων Εισόδου (Login Class)

Η μέθοδος αυτή επιτρέπει να γίνει η ρύθμιση των μεταβλητών περιβάλλοντος μια φορά για κάθε κέλυφος, αντί να χρειάζεται να τεθούν συγκεκριμένες τιμές στο αρχείο εκκίνησης του καθενός

χωριστά. Οι Ρυθμίσεις σε Επίπεδο Χρήστη μπορούν να γίνουν από τον ίδιο το χρήστη, ενώ οι Ρυθμίσεις σε Επίπεδο Διαχειριστή απαιτούν προνόμια υπερχρήστη.

43.3.4.1.1.1. Ρυθμίσεις σε Επίπεδο Χρήστη

Το παρακάτω απλό παράδειγμα, δείχνει ένα αρχείο .login_conf στον κατάλογο κάποιου χρήστη στο οποίο και οι δύο μεταβλητές έχουν τεθεί για κωδικοποίηση Latin-1:

```
me:\
    :charset=ISO-8859-1:\
    :lang=de_DE.ISO8859-1:
```

Παρακάτω βλέπετε ένα .login_conf στο οποίο οι μεταβλητές έχουν τεθεί για Παραδοσιακά Κινέζικα σε κωδικοποίηση BIG-5. Παρατηρήστε ότι έχουμε θέσει πολύ περισσότερες μεταβλητές, καθώς κάποιες εφαρμογές δεν σέβονται σωστά τις μεταβλητές για Κινέζικα, Γιαπωνέζικα και Κορεάτικα.

```
#Users who do not wish to use monetary units or time formats
#of Taiwan can manually change each variable
me:\
    :lang=zh_TW.Big5:\
    :setenv=LC_ALL=zh_TW.Big5:\
    :setenv=LC_COLLATE=zh_TW.Big5:\
    :setenv=LC_CTYPE=zh_TW.Big5:\
    :setenv=LC_MESSAGES=zh_TW.Big5:\
    :setenv=LC_MONETARY=zh_TW.Big5:\
    :setenv=LC_NUMERIC=zh_TW.Big5:\
    :setenv=LC_TIME=zh_TW.Big5:\
    :charset=big5:\
    :xmodifiers="@im=gcin": #Set gcin as the XIM Input Server
```

Για περισσότερες πληροφορίες, δείτε τις Ρυθμίσεις σε Επίπεδο Διαχειριστή και την login.conf(5).

43.3.4.1.2. Ρυθμίσεις σε Επίπεδο Διαχειριστή

Βεβαιωθείτε ότι έχει οριστεί η σωστή γλώσσα στην κλάση του χρήστη, στο αρχείο /etc/login.conf. Στο αρχείο αυτό θα πρέπει να υπάρχουν οι παρακάτω ρυθμίσεις:

```
language_name|Account Type Description:\
    :charset=MIME_charset:\
    :lang=locale_name:\
    :tc=default:
```

Με βάση το προηγούμενο παράδειγμα μας που χρησιμοποιήσαμε Latin-1, το αρχείο θα μοιάζει με το παρακάτω:

```
german|German Users Accounts:\
    :charset=ISO-8859-1:\
```

```
    :lang=de_DE.ISO8859-1:\
    :tc=default:
```

Πριν κάνετε αλλαγές στις Κλάσεις Εισόδου (Login Classes) των χρηστών, εκτελέστε την παρακάτω εντολή:

```
# cap_mkdb /etc/login.conf
```

ώστε να ενεργοποιηθούν στο σύστημα οι αλλαγές που κάνατε στο /etc/login.conf.

43.3.4.1.3. Αλλαγή Κλάσεων Εισόδου μέσω της vipw(8)

Χρησιμοποιήστε την `vipw` για να προσθέσετε νέους χρήστες, και κάντε την καταχώριση να μοιάζει με την παρακάτω:

```
user:password:1111:11:language:0:0:User Name:/home/user:/bin/sh
```

43.3.4.1.4. Αλλαγή Κλάσεων Εισόδου μέσω της adduser(8)

Χρησιμοποιήστε την `adduser` για να προσθέσετε νέους χρήστες, και έπειτα ακολουθήστε τις παρακάτω οδηγίες:

- Θέστε το `defaultclass = language` στο /etc/adduser.conf. Να έχετε υπόψη σας ότι σε αυτή την περίπτωση, θα πρέπει να ορίσετε μια κλάση `default` για όλους τους χρήστες άλλων γλωσσών.
- Μια εναλλακτική λύση, είναι να απαντάτε κάθε φορά στην ερώτηση

  ```
  Enter login class: default []:
  ```

  που εμφανίζεται από την adduser(8).

- Ακόμα μια εναλλακτική λύση, είναι να χρησιμοποιήσετε το παρακάτω σε κάθε χρήστη που θέλετε να προσθέσετε και ο οποίος χρησιμοποιεί διαφορετική γλώσσα:

  ```
  # adduser -class language
  ```

43.3.4.1.5. Αλλαγή Κλάσεων Εισόδου μέσω της pw(8)

Αν χρησιμοποιείτε την pw(8) για να προσθέσετε νέους χρήστες, καλέστε την με τον παρακάτω τρόπο:

```
# pw useradd user_name -L language
```

43.3.4.1.6. Μέθοδος Αρχείων Εκκίνησης Κελύφους

Η μέθοδος αυτή δεν συνίσταται, καθώς απαιτεί διαφορετικές ρυθμίσεις για κάθε διαφορετικό πρόγραμμα κελύφους που χρησιμοποιείται. Προτιμήστε καλύτερα την μέθοδο των Κλάσεων Εισόδου.

Για να προσθέσετε τις τοπικές ρυθμίσεις και το σετ χαρακτήρων MIME, ρυθμίστε απλώς τις δύο μεταβλητές περιβάλλοντος που φαίνονται παρακάτω στο αρχείο /etc/profile ή/και στο /etc/csh.login. Θα χρησιμοποιήσουμε τα Γερμανικά ως γλώσσα για το παρακάτω παράδειγμα:

Στο /etc/profile:

```
LANG=de_DE.ISO8859-1; export LANG
MM_CHARSET=ISO-8859-1; export MM_CHARSET
```

Ή στο /etc/csh.login:

```
setenv LANG de_DE.ISO8859-1
setenv MM_CHARSET ISO-8859-1
```

Εναλλακτικά, μπορείτε να προσθέσετε τις παραπάνω οδηγίες στο /usr/shared/skel/dot.profile (αντίστοιχα με τις οδηγίες για το /etc/profile που είδαμε παραπάνω), ή στο /usr/shared/skel/dot.login (αντίστοιχα με τις οδηγίες για το /etc/csh.login που είδαμε επίσης παραπάνω).

Για το X11:

Στο $HOME/.xinitrc:

```
LANG=de_DE.ISO8859-1; export LANG
```

Ή:

```
setenv LANG de_DE.ISO8859-1
```

Ανάλογα με το κέλυφος που χρησιμοποιείτε (δείτε παραπάνω).

43.3.5. Ρυθμίσεις για την Κονσόλα

Για όλα τα single C σετ χαρακτήρων, μπορείτε να θέσετε τις γραμματοσειρές της κονσόλας στο /etc/rc.conf για την επιθυμητή γλώσσα, γράφοντας:

```
font8x16=font_name
font8x14=font_name
font8x8=font_name
```

Το *font_name* εδώ προκύπτει από το αντίστοιχο αρχείο του καταλόγου /usr/shared/syscons/fonts, αφαιρώντας την κατάληξη .fnt.

Αν χρειάζεται, χρησιμοποιήστε την κατάλληλη αντιστοίχηση πληκτρολογίου (keymap) και οθόνης για το σετ χαρακτήρων single C που χρησιμοποιείτε, μέσω του `sysinstall`. Μόλις εκτελέσετε το sysinstall, επιλέξτε το Configure, και έπειτα το Console. Εναλλακτικά, μπορείτε να προσθέσετε το παρακάτω στο /etc/rc.conf:

```
scrnmap=screenmap_name
keymap=keymap_name
keychange="fkey_number sequence"
```

Στην περίπτωση αυτή, το *screenmap_name* προέρχεται από ένα αρχείο του καταλόγου /usr/shared/syscons/scrnmaps, χωρίς την κατάληξη .scm. Η αντιστοίχηση οθόνης μαζί με την αντίστοιχη γραμματοσειρά, χρησιμοποιείται συνήθως για την επέκταση του 8ου bit στο 9ο, για κάρτες VGA που χρησιμοποιούν μήτρα χαρακτήρων με 8 στήλες.

Αν έχετε ενεργοποιημένο τον δαίμονα moused στο αρχείο /etc/rc.conf:

```
moused_enable="YES"
```

καλό θα είναι να εξετάσετε τις πληροφορίες σχετικά με τον δρομέα του ποντικιού που εμφανίζονται στην παρακάτω παράγραφο.

Ο προεπιλεγμένος δρομέας του ποντικιού που χρησιμοποιείται από το πρόγραμμα οδήγησης syscons(4), καταλαμβάνει τις θέσεις 0xd0-0xd3 του συνόλου χαρακτήρων. Αν αυτή η περιοχή χαρακτήρων δεν είναι διαθέσιμη στη γλώσσα που χρησιμοποιείτε, θα πρέπει να μετακινήσετε την περιοχή του δρομέα έξω από αυτήν. Για να γίνει αυτό στο FreeBSD, προσθέστε την ακόλουθη γραμμή στο /etc/rc.conf:

```
mousechar_start=3
```

Το *keymap_name* προέρχεται από ένα αρχείο του καταλόγου /usr/shared/syscons/keymaps, χωρίς την κατάληξη .kbd. Αν δεν είστε σίγουρος για την αντιστοίχηση πληκτρολογίου που χρειάζεται να χρησιμοποιήσετε, μπορείτε να χρησιμοποιήσετε το kbdmap(1) για να κάνετε δοκιμές σε διάφορες αντιστοιχίσεις, χωρίς να χρειάζεται να κάνετε επανεκκίνηση.

Η λειτουργία `keychange` χρησιμοποιείται συνήθως για τον προγραμματισμό των πλήκτρων λειτουργιών (function keys), ώστε να ταιριάζουν με τον επιλεγμένο τύπο τερματικού, καθώς οι ακολουθίες των πλήκτρων λειτουργιών δεν μπορούν να καθοριστούν στις αντιστοιχίσεις πληκτρολογίου.

Βεβαιωθείτε επίσης ότι έχετε ρυθμίσει το σωστό τύπου τερματικού στο /etc/ttys για όλες τις καταχωρίσεις `ttyv*`. Τη δεδομένη στιγμή, οι προκαθορισμένες αντιστοιχίες είναι:

Σετ Χαρακτήρων	Τύπος Τερματικού
ISO8859-1 ή ISO8859-15	cons25l1
ISO8859-2	cons25l2
ISO8859-7	cons25l7
KOI8-R	cons25r
KOI8-U	cons25u
CP437 (προεπιλεγμένο VGA)	cons25
US-ASCII	cons25w

Για γλώσσες με χαρακτήρες wide ή multibyte, χρησιμοποιήστε το σωστό FreeBSD port στον κατάλογο /usr/ports/language. Μερικές θύρες εμφανίζονται ως κονσόλα, ενώ το σύστημα τις βλέπει ως σειριακά vtty, και έτσι πρέπει να παρακρατήσετε αρκετά vtty, τόσο για το X11 όσο και για την ψευτό-σειριακή κονσόλα. Παρακάτω θα βρείτε μια μερικώς ενημερωμένη λίστα για χρήση άλλων γλωσσών στην κονσόλα:

Γλώσσα	Τοποθεσία
Παραδοσιακά Κινέζικα (BIG-5)	chinese/big5con
Γιαπωνέζικα	japanese/kon2-16dot ή japanese/mule-freewnn
Κορεάτικα	korean/han

43.3.6. Ρύθμιση του X11

Αν και το X11 δεν είναι μέρος του FreeBSD Project, θα δώσουμε εδώ κάποιες χρήσιμες πληροφορίες για όσους το χρησιμοποιούν στο FreeBSD. Για περισσότερες πληροφορίες, δείτε την δικτυακή τοποθεσία του Xorg, ή του εξυπηρετητή X11 που πρόκειται να χρησιμοποιήσετε.

Στο αρχείο ~/.Xresources, μπορείτε επιπρόσθετα να αλλάξετε και άλλες ρυθμίσεις που σχετίζονται με το I18N (π.χ. γραμματοσειρές, μενού, κ.λ.π.).

43.3.6.1. Απεικόνιση Γραμματοσειρών

Εγκαταστήστε τον εξυπηρετητή Xorg (x11-servers/xorg-server) και έπειτα εγκαταστήστε τις γραμματοσειρές TrueType® για την επιθυμητή γλώσσα. Με τις σωστές τοπικές ρυθμίσεις, θα μπορείτε να δείτε την επιλεγμένη γλώσσα στα μενού και τα μηνύματα του γραφικού περιβάλλοντος.

43.3.6.2. Εισαγωγή μη-Αγγλικών Χαρακτήρων

Η μέθοδος εισόδου X11 (XIM, X11 Input Method), είναι ένα νέο πρότυπο για όλους τους πελάτες X11. Όλες οι εφαρμογές του X11 θα πρέπει να γράφονται ως πελάτες του XIM, και να λαμβάνουν είσοδο από εξυπηρετητές εισόδου XIM. Υπάρχουν διαθέσιμοι διάφοροι εξυπηρετητές XIM, για διαφορετικές γλώσσες.

43.3.7. Ρύθμιση Εκτυπωτή

Κάποια σετ χαρακτήρων single C είναι συνήθως ενσωματωμένα στο ίδιο το υλικό των εκτυπωτών. Τα σετ χαρακτήρων τύπου wide ή multibyte απαιτούν ειδικές ρυθμίσεις, και συνιστούμε να χρησιμοποιήσετε το apsfilter. Μπορείτε επίσης να μετατρέψετε το έγγραφο σας σε PostScript® ή PDF, χρησιμοποιώντας εργαλεία ειδικά φτιαγμένα για τη συγκεκριμένη γλώσσα.

43.3.8. Πυρήνας και Συστήματα Αρχείων

Το σύστημα αρχείων FFS (fast filesystem) του FreeBSD μπορεί να διαχειριστεί ονόματα αρχείων που ανήκουν σε σετ single C (είναι 8-bit clean, δείτε και το multibyte(3)), αλλά δεν αποθηκεύει το σετ χαρακτήρων που χρησιμοποιείται. Με άλλα λόγια, είναι 8-bit αλλά δεν γνωρίζει τίποτα για την κωδικοποίηση των χαρακτήρων. Επίσημα, το FFS δεν υποστηρίζει ακόμα σετ χαρακτήρων wide ή multibyte. Υπάρχουν ωστόσο κάποια ανεξάρτητα patches για το FFS που υποστηρίζουν αυτές τις δυνατότητες. Πρόκειται μόνο για προσωρινές και μη μεταφέρσιμες λύσεις ή hacks, και έχουμε αποφασίσει να μην τα περιλάβουμε στο κεντρικό δέντρο πηγαίου κώδικα. Δείτε τις ιστοσελίδες των αντίστοιχων γλωσσών για περισσότερες πληροφορίες και για να ανακτήσετε τα απαραίτητα αρχεία.

Το σύστημα αρχείων MS-DOS® στο FreeBSD έχει την δυνατότητα να ρυθμιστεί ώστε να μετατρέπει μεταξύ των σετ χαρακτήρων Unicode, του MS-DOS®, και του σετ χαρακτήρων που έχει επιλεγεί για το σύστημα αρχείων του FreeBSD. Για περισσότερες λεπτομέρειες, δείτε τη σελίδα manual mount_msdosfs(8).

43.4. Μεταγλώττιση Προγραμμάτων I18N

Πολλά ports του FreeBSD διαθέτουν υποστήριξη I18N. Σε μερικά από αυτά, το -I18N είναι μέρος του ονόματος τους. Τα προγράμματα αυτά, και πολλά περισσότερα, έχουν ενσωματωμένη υποστήριξη για I18N και δεν χρειάζονται άλλες ειδικές ρυθμίσεις.

Ωστόσο, σε κάποιες εφαρμογές όπως η MySQL, θα πρέπει να ρυθμιστεί το Makefile με το επιθυμητό σετ χαρακτήρων. Αυτό συνήθως γίνεται περνώντας μια τιμή στο configure στον πηγαίο κώδικα, ή αλλάζοντας το ίδιο το Makefile.

43.5. Τοπικές Ρυθμίσεις για Συγκεκριμένες Γλώσσες

43.5.1. Ρώσικη Γλώσσα (Κωδικοποίηση KOI8-R)

Για περισσότερες πληροφορίες σχετικά με την κωδικοποίηση KOI8-R, δείτε τις Αναφορές Σχετικά με το Σετ Χαρακτήρων KOIR-8 (Ρωσικό Σύνολο Χαρακτήρων).

43.5.1.1. Τοπικές Ρυθμίσεις

Τοποθετήστε τις ακόλουθες γραμμές στο αρχείο σας ~/.login_conf:

```
me:My Account:\
    :charset=KOI8-R:\
    :lang=ru_RU.KOI8-R:
```

Για παραδείγματα που σχετίζονται με τις Τοπικές Ρυθμίσεις, δείτε προηγούμενες ενότητες σε αυτό το κεφάλαιο.

43.5.1.2. Ρύθμιση Κονσόλας

- Προσθέστε την ακόλουθη γραμμή στο αρχείο /etc/rc.conf:

```
mousechar_start=3
```

- Χρησιμοποιήστε επίσης τις παρακάτω ρυθμίσεις στο /etc/rc.conf:

```
keymap="ru.utf-8"
scrnmap="utf-82cp866"
font8x16="cp866b-8x16"
font8x14="cp866-8x14"
font8x8="cp866-8x8"
```

- Για κάθε καταχώριση `ttyv*` στο αρχείο /etc/ttys, χρησιμοποιήστε το `cons25r` ως τύπο τερματικού.

Για παραδείγματα που σχετίζονται με την ρύθμιση της κονσόλας, δείτε προηγούμενες ενότητες αυτού του κεφαλαίου.

43.5.1.3. Ρύθμιση Εκτυπωτή

Καθώς οι περισσότεροι εκτυπωτές που διαθέτουν Ρωσικούς χαρακτήρες έχουν ενσωματωμένη την κωδικοσελίδα CP866, θα χρειαστείτε ειδικό φίλτρο εξόδου για να μετατρέψετε από το KOI8-R στο CP866. Το φίλτρο αυτό εγκαθίσταται από προεπιλογή στο /usr/libexec/lpr/ru/koi2alt. Η καταχώριση για ένα Ρώσικο εκτυπωτή στο /etc/printcap θα μοιάζει με την παρακάτω:

```
lp|Russian local line printer:\
    :sh:of=/usr/libexec/lpr/ru/koi2alt:\
    :lp=/dev/lpt0:sd=/var/spool/output/lpd:lf=/var/log/lpd-errs:
```

Δείτε το printcap(5) για πιο λεπτομερή περιγραφή.

43.5.1.4. Σύστημα Αρχείων MS-DOS® και Ρώσικα Ονόματα Αρχείων

Το παρακάτω υπόδειγμα καταχώρισης στο fstab(5) ενεργοποιεί την υποστήριξη για Ρώσικα ονόματα αρχείων σε προσαρτημένα συστήματα αρχείων τύπου MS-DOS®:

```
/dev/ad0s2      /dos/c  msdos   rw,-Wkoi2dos,-Lru_RU.KOI8-R 0 0
```

Η επιλογή `-L` επιλέγει τις τοπικές ρυθμίσεις που θα χρησιμοποιηθούν, και η `-W` ορίζει τον πίνακα μετατροπής χαρακτήρων. Για να χρησιμοποιήσετε την επιλογή `-W` βεβαιωθείτε ότι έχετε προσαρτήσει την κατάτμηση /usr πριν την κατάτμηση MS-DOS®, καθώς οι πίνακες μετατροπής βρίσκονται στο /usr/libdata/msdosfs. Για περισσότερες πληροφορίες, δείτε τη σελίδα manual του

mount_msdosfs(8).

43.5.1.5. Ρύθμιση X11

1. Εκτελέστε πρώτα τις γενικές τοπικές ρυθμίσεις που έχουμε ήδη περιγράψει.
2. Αν χρησιμοποιείτε τον εξυπηρετητή Xorg, εγκαταστήστε το πακέτο x11-fonts/xorg-fonts-cyrillic.

   Ελέγξτε την ενότητα `"Files"` στο αρχείο /etc/X11/xorg.conf. Θα πρέπει να προσθέσετε την παρακάτω γραμμή *πριν* από οποιαδήποτε άλλη καταχώριση `FontPath`:

   ```
   FontPath   "/usr/local/lib/X11/fonts/cyrillic"
   ```

   Δείτε στην Συλλογή των Ports για περισσότερες κυριλλικές γραμματοσειρές.
3. Για την ενεργοποίηση του Ρωσικού πληκτρολογίου, προσθέστε τις παρακάτω γραμμές στην ενότητα `"Keyboard"` του αρχείου xorg.conf:

   ```
   Option "XkbLayout"   "us,ru"
   Option "XkbOptions"  "grp:toggle"
   ```

   Βεβαιωθείτε επίσης ότι η γραμμή `XkbDisable` είναι ανενεργή (μαρκαρισμένη ως σχόλιο).

   Αν χρησιμοποιήσετε το `grp:toggle` η εναλλαγή RUS/LAT θα γίνεται με το `Δεξι ό Alt`, ενώ αν θέσετε `grp:ctrl_shift_toggle`, η εναλλαγή θα γίνεται με το `Ctrl` + `Shift`. Για `grp:caps_toggle`, η εναλλαγή RUS/LAT θα γίνεται με το `CapsLock`. Η κανονική λειτουργία του `CapsLock` εξακολουθεί να είναι διαθέσιμη μέσω του συνδυασμού πλήκτρων `Shift` + `CapsLock` (μόνο σε κατάσταση LAT). Το `grp:caps_toggle` για κάποιο άγνωστο λόγο, δεν λειτουργεί στο Xorg.

   Αν το πληκτρολόγιο σας διαθέτει πλήκτρα "Windows®", και έχετε παρατηρήσει ότι κάποια από τα μη-αλφαριθμητικά πλήκτρα έχουν λάθος αντιστοίχηση όταν είστε σε κατάσταση RUS, προσθέστε την παρακάτω γραμμή στο αρχείο xorg.conf:

   ```
   Option "XkbVariant" ",winkeys"
   ```

   Το Ρώσικο XKB πληκτρολόγιο ίσως δεν λειτουργεί με εφαρμογές που δεν έχουν φτιαχτεί για τις αντίστοιχες τοπικές ρυθμίσεις.

Οι εφαρμογές που τηρούν τις ελάχιστες προδιαγραφές τοπικών ρυθμίσεων, θα πρέπει να καλούν από νωρίς τη συνάρτηση `XtSetLanguageProc (NULL, NULL, NULL);` μέσα στον κώδικα τους.

Δείτε το KOI8-R για το σύστημα X Window για περισσότερες οδηγίες σχετικά με την δημιουργία εφαρμογών X11 που να χρησιμοποιούν τοπικές ρυθμίσεις.

43.5.2. Τοπικές Ρυθμίσεις για Παραδοσιακά Κινέζικα Ταϊβάν

Το FreeBSD-Taiwan Project έχει δημιουργήσει ένα HOWTO για τα Κινέζικα στο FreeBSD, το οποίο μπορείτε να βρείτε στη διεύθυνση http://netlab.cse.yzu.edu.tw/~statue/freebsd/zh-tut/, χρησιμοποιώντας πολλά Κινέζικα ports. Ο τρέχων συντάκτης του `Κινέζικου FreeBSD Howto` είναι ο Shen Chuan-Hsing statue@freebsd.sinica.edu.tw.

Ο Chuan-Hsing Shen statue@freebsd.sinica.edu.tw έχει δημιουργήσει την Κινέζικη Συλλογή FreeBSD (CFC) χρησιμοποιώντας την κωδικοποίηση `zh-L10N-tut` του FreeBSD-Ταΐβάν. Τα πακέτα και τα scripts διατίθενται στη διεύθυνση ftp://freebsd.csie.nctu.edu.tw/pub/taiwan/CFC/.

43.5.3. Τοπικές Ρυθμίσεις για την Γερμανική Γλώσσα (για Όλες τις Γλώσσες που Βασίζονται στο ISO 8859-1)

Ο Slaven Rezic eserte@cs.tu-berlin.de έχει γράψει ένα οδηγό για την χρήση των umlauts σε ένα μηχάνημα FreeBSD. Ο οδηγός είναι γραμμένος στα Γερμανικά και διατίθεται στην τοποθεσία http://user.cs.tu-berlin.de/~eserte/FreeBSD/doc/umlaute/umlaute.html.

43.5.4. Τοπικές Ρυθμίσεις για την Ελληνική Γλώσσα

Ο Nikos Kokkalis <nickkokkalis@gmail.com> έχει γράψει ένα πλήρες άρθρο για την υποστήριξη της Ελληνικής γλώσσας στο FreeBSD. Το άρθρο αυτό διατίθεται ως μέρος της επίσημης Ελληνικής τεκμηρίωσης του FreeBSD, στην τοποθεσία Υποστήριξη της Ελληνικής Γλώσσας στο FreeBSD.

43.5.5. Τοπικές Ρυθμίσεις Για Γιαπωνέζικα και Κορεάτικα

Για Γιαπωνέζικα, δείτε στην τοποθεσία http://www.jp.FreeBSD.org/, ενώ για Κορεάτικα, δείτε στην τοποθεσία http://www.kr.FreeBSD.org/.

43.5.6. Τεκμηρίωση του FreeBSD σε Γλώσσες Εκτός της Αγγλικής

Κάποιοι εθελοντές του FreeBSD έχουν μεταφράσει τμήματα της τεκμηρίωσης του σε άλλες γλώσσες. Οι μεταφράσεις αυτές διατίθενται μέσω συνδέσμων στην κύρια δικτυακή τοποθεσία του FreeBSD ή στον κατάλογο /usr/shared/doc.

Chapter 44. Ενημέρωση και Αναβάθμιση του FreeBSD

44.1. Σύνοψη

Το FreeBSD βρίσκεται υπό συνεχή εξέλιξη μεταξύ των επίσημων εκδόσεων του. Μερικοί άνθρωποι προτιμούν να χρησιμοποιούν τις επίσημες εκδόσεις, ενώ άλλοι προτιμούν να κρατούν το σύστημα τους ενημερωμένο με τις τελευταίες εξελίξεις. Ωστόσο, ακόμα και οι επίσημες εκδόσεις ενημερώνονται συχνά με διορθώσεις κρίσιμων σφαλμάτων και ασφαλείας. Όποια έκδοση και να χρησιμοποιήσετε, το FreeBSD παρέχει όλα τα απαραίτητα εργαλεία για να κρατήσετε το σύστημα σας ενημερωμένο, και επίσης σας επιτρέπει να αναβαθμιστείτε εύκολα σε κάποια επόμενη έκδοση. Το κεφάλαιο αυτό θα σας βοηθήσει να αποφασίσετε αν θέλετε να παρακολουθείτε το σύστημα ανάπτυξης, ή αν θα προτιμήσετε να παραμείνετε σε μια από τις παγιωμένες εκδόσεις. Θα παρουσιάσουμε επίσης τα βασικά εργαλεία που απαιτούνται για την ενημέρωση και αναβάθμιση του συστήματος.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Ποια βοηθητικά προγράμματα μπορείτε να χρησιμοποιήσετε για να ενημερώσετε το σύστημα και την Συλλογή των Ports.
- Πως να διατηρείτε το σύστημα σας ενημερωμένο με τα προγράμματα freebsd-updateCVSup, CVS, ή CTM.
- Πως να συγκρίνετε την κατάσταση ενός εγκατεστημένου συστήματος, με αναφορά ένα γνωστό και εγγυημένα σωστό σύστημα.
- Πως να διατηρήσετε την τεκμηρίωση σας ενημερωμένη μέσω του CVSup ή των ports της τεκμηρίωσης .
- Τη διαφορά μεταξύ των δύο κλάδων που βρίσκονται σε εξέλιξη: του FreeBSD-STABLE και του FreeBSD-CURRENT.
- Πως να ξαναφτιάξετε και να επανεγκαταστήσετε ολόκληρο το βασικό σύστημα με την `make buildworld` (κλπ).

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ρυθμίσετε σωστά τη σύνδεση σας στο δίκτυο (Προχωρημένα Θέματα Δικτύωσης).
- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

Στο κεφάλαιο αυτό γίνεται συχνά χρήση της εντολής `cvsup` για την ανάκτηση ή ενημέρωση των αρχείων πηγαίου κώδικα του FreeBSD. Για να την χρησιμοποιήσετε, θα πρέπει να εγκαταστήσετε ένα πακέτο ή port όπως το net/cvsup (αν δεν θέλετε να εγκαταστήσετε γραφικό πρόγραμμα `cvsup`, μπορείτε να εγκαταστήσετε το port net/cvsup-without-gui). Μπορείτε να αντικαταστήσετε αυτή την εντολή με την csup(1) η οποία ανήκει στο βασικό σύστημα.

44.2. Ενημερώνοντας το FreeBSD

Η εφαρμογή ενημερώσεων ασφαλείας αποτελεί ένα σημαντικό τμήμα της συντήρησης λογισμικού, ειδικά όταν πρόκειται για το λειτουργικό σύστημα. Για μεγάλο διάστημα, η διαδικασία αυτή δεν ήταν εύκολη στο FreeBSD. Έπρεπε να εφαρμοστούν patches στον πηγαίο κώδικα, να γίνει μεταγλώττιση του από την αρχή, και να εγκατασταθούν ξανά τα νέα εκτελέσιμα.

Αυτό δεν είναι πλέον αναγκαίο, καθώς το FreeBSD διαθέτει τώρα ένα βοηθητικό πρόγραμμα, το `freebsd-update`. Το πρόγραμμα παρέχει δύο διαφορετικές λειτουργίες. Η πρώτη είναι η δυνατότητα δυαδικής (binary) ενημέρωσης του βασικού συστήματος με τις τελευταίες διορθώσεις ασφάλειας και λαθών, χωρίς να χρειάζεται ξανά μεταγλώττιση και εγκατάσταση. Η δεύτερη είναι η δυνατότητα αναβάθμισης του συστήματος σε μια νέα μικρή ή μεγάλη επίσημη έκδοση (release).

Δυαδικές διορθώσεις λαθών και ασφάλειας, διατίθενται για όλες τις αρχιτεκτονικές και εκδόσεις που υποστηρίζονται από την ομάδα ασφάλειας. Πριν προχωρήσετε στην αναβάθμιση σε μια νέα έκδοση, θα πρέπει να διαβάσετε τις σχετικές με αυτήν ανακοινώσεις, καθώς μπορεί να περιέχουν σημαντικές πληροφορίες. Μπορείτε να δείτε τις ανακοινώσεις εκδόσεων στην παρακάτω τοποθεσία: http://www.FreeBSD.org/releases/.

Αν υπάρχει κάποιο `crontab` που χρησιμοποιεί τις δυνατότητες του `freebsd-update`, θα πρέπει να απενεργοποιηθεί πριν ξεκινήσει η παρακάτω διαδικασία. Μπορείτε να εγκαταστήσετε την τελευταία έκδοση του `freebsd-update` κατεβάζοντας το συμπιεσμένο πακέτο από το παραπάνω URL και εκτελώντας τις παρακάτω εντολές:

```
# gunzip -c freebsd-update-upgrade.tgz | tar xvf -
# mv freebsd-update.sh /usr/sbin/freebsd-update
# mv freebsd-update.conf /etc
```

Δεν απαιτείται να κατεβάσετε την τελευταία έκδοση, αν χρησιμοποιείτε κάποια από τις τρέχουσες εκδόσεις του FreeBSD.

44.2.1. Το Αρχείο Ρυθμίσεων

Κάποιοι χρήστες ίσως θέλουν να αλλάξουν το προεπιλεγμένο αρχείο ρυθμίσεων /etc/freebsd-update.conf, ώστε να έχουν καλύτερο έλεγχο της διαδικασίας. Οι επιλογές είναι γενικά αρκετά καλά τεκμηριωμένες, αλλά οι παρακάτω ίσως να χρειάζονται κάποιες επιπλέον επεξηγήσεις:

```
# Components of the base system which should be kept updated.
Components src world kernel
```

Αυτή η παράμετρος ελέγχει ποια τμήματα του FreeBSD θα διατηρούνται ενημερωμένα. Η προεπιλογή είναι να ενημερώνεται ο πηγαίος κώδικας, όλο το βασικό σύστημα, και ο πυρήνας. Τα τμήματα είναι τα ίδια που διατίθενται και κατά την εγκατάσταση, για παράδειγμα αν βάλετε την επιλογή `world/games` θα εγκαθίστανται ενημερώσεις για τα παιχνίδια. Αν βάλετε `src/bin` θα επιτρέψετε την ενημέρωση του πηγαίου κώδικα του καταλόγου src/bin.

Η καλύτερη επιλογή είναι να αφήσετε εδώ την προεπιλεγμένη τιμή, καθώς αν την αλλάξετε ώστε να περιέχει συγκεκριμένα μόνο τμήματα, θα αναγκαστείτε να αναφέρετε χωριστά μέσα στο αρχείο ρυθμίσεων κάθε τμήμα που θέλετε να ενημερώνεται. Αυτό ίσως έχει καταστροφικά αποτελέσματα, καθώς είναι πιθανό ο πηγαίος κώδικας και τα εκτελέσιμα προγράμματα να μην είναι πλέον σε συγχρονισμό μεταξύ τους.

```
# Paths which start with anything matching an entry in an IgnorePaths
# statement will be ignored.
IgnorePaths
```

Προσθέστε διαδρομές σε καταλόγους, όπως /bin ή /sbin για να αφήσετε απείραχτους τους συγκεκριμένους καταλόγους κατά την διαδικασία ενημέρωσης. Η επιλογή αυτή μπορεί να χρησιμοποιηθεί για να αποτρέψει το `freebsd-update` να γράψει πάνω σε πιθανόν δικές σας τοπικές αλλαγές.

```
# Paths which start with anything matching an entry in an UpdateIfUnmodified
# statement will only be updated if the contents of the file have not been
# modified by the user (unless changes are merged; see below).
UpdateIfUnmodified /etc/ /var/ /root/ /.cshrc /.profile
```

Η επιλογή αυτή θα ενημερώσει τα αρχεία ρυθμίσεων στους καταλόγους που καθορίζονται, μόνο αν αυτά δεν έχουν μεταβληθεί από το χρήστη. Αν υπάρχουν τοπικές αλλαγές, δεν θα γίνει ενημέρωση. Υπάρχει μια ακόμα επιλογή, η `KeepModifiedMetadata`, η οποία οδηγεί το `freebsd-update` να αποθηκεύσει τις αλλαγές μεταξύ των δύο εκδόσεων κατά τη διάρκεια της συγχώνευσης (merge).

```
# When upgrading to a new FreeBSD release, files which match MergeChanges
# will have any local changes merged into the version from the new release.
MergeChanges /etc/ /var/named/etc/
```

Πρόκειται για τη λίστα των καταλόγων που περιέχουν αρχεία ρυθμίσεων, και στα οποία το `freebsd-update` θα επιχειρεί την διαδικασία συγχώνευσης αλλαγών. Η διαδικασία συγχώνευσης γίνεται με μια σειρά από patches τύπου diff(1) παρόμοια με το mergemaster(8) αλλά με λιγότερες επιλογές. Οι συγχωνεύσεις είτε γίνονται δεκτές, είτε προκαλούν το άνοιγμα κάποιου συντάκτη κειμένου, διαφορετικά η εκτέλεση του `freebsd-update` ακυρώνεται. Αν δεν είστε σίγουρος, κρατήστε αντίγραφο ασφαλείας του καταλόγου /etc και απλώς δεχθείτε τις αλλαγές. Δείτε το `mergemaster` για περισσότερες πληροφορίες σχετικά με την εντολή `mergemaster`.

```
# Directory in which to store downloaded updates and temporary
# files used by FreeBSD Update.
# WorkDir /var/db/freebsd-update
```

Στον κατάλογο αυτό φυλάσσονται όλα τα patches και τα προσωρινά αρχεία. Σε περιπτώσεις όπου ο χρήστης εκτελεί αναβάθμιση σε μια νεότερη έκδοση του FreeBSD, θα πρέπει να διαθέτει τουλάχιστον ένα gigabyte ελεύθερου χώρου.

```
# When upgrading between releases, should the list of Components be
# read strictly (StrictComponents yes) or merely as a list of components
# which *might* be installed of which FreeBSD Update should figure out
# which actually are installed and upgrade those (StrictComponents no)?
# StrictComponents no
```

Αν θέσετε την παραπάνω επιλογή στο `yes`, το `freebsd-update` θα υποθέσει ότι η λίστα `Components` είναι πλήρης και δεν θα επιχειρήσει να προχωρήσει σε αλλαγές εκτός λίστας. Ουσιαστικά, το `freebsd-update` θα προσπαθήσει να ενημερώσει κάθε αρχείο που ανήκει στη λίστα `Components`.

44.2.2. Patches Σχετικά με την Ασφάλεια

Τα patches που σχετίζονται με την ασφάλεια, αποθηκεύονται σε ένα απομακρυσμένο μηχάνημα και μπορούν να μεταφορτωθούν και να εγκατασταθούν με την ακόλουθη εντολή:

```
# freebsd-update fetch
# freebsd-update install
```

Αν με την παραπάνω εντολή εγκατασταθούν ενημερώσεις στον πυρήνα, θα χρειαστεί να επανεκκινήσετε το σύστημα. Αν όλα πάνε καλά, το σύστημα θα είναι πλέον ενημερωμένο και μπορείτε να εκτελείτε το `freebsd-update` αυτόματα με την βοήθεια του cron(8). Μια απλή καταχώριση στο αρχείο /etc/crontab είναι επαρκής για αυτό το σκοπό:

```
@daily                                  root    freebsd-update cron
```

Η παραπάνω καταχώριση ορίζει ότι το `freebsd-update` θα εκτελείται μια φορά την ημέρα. Με τον τρόπο αυτό, και όταν η εκτέλεση είναι μέσω της επιλογής `cron`, το `freebsd-update` απλώς θα ελέγχει για ενημερώσεις. Αν υπάρχουν, η εφαρμογή θα τις κατεβάζει, αλλά δεν θα τις εγκαθιστά. Θα στέλνει όμως ένα email στο χρήστη `root` ώστε να τις εγκαταστήσει χειροκίνητα.

Αν οτιδήποτε πάει στραβά, το `freebsd-update` έχει την ικανότητα να επιστρέφει στην προηγούμενη σταθερή κατάσταση, αναιρώντας το τελευταίο σετ αλλαγών με την ακόλουθη εντολή:

```
# freebsd-update rollback
```

Με την ολοκλήρωση της εντολής, θα πρέπει να επανεκκινήσετε το σύστημα αν έχουν γίνει αλλαγές στον πυρήνα ή σε κάποιο από τα αρθρώματα του. Αυτό θα επιτρέψει στο FreeBSD να φορτώσει τα νέα εκτελέσιμα στη μνήμη.

Το βοηθητικό πρόγραμμα `freebsd-update` μπορεί να ενημερώσει αυτόματα μόνο τον πυρήνα GENERIC. Αν χρησιμοποιείται προσαρμοσμένος πυρήνας, θα πρέπει να μεταγλωττιστεί ξανά, όταν το `freebsd-update` τελειώσει με την εγκατάσταση των υπόλοιπων ενημερώσεων. Ωστόσο, το `freebsd-update` θα ανιχνεύσει και θα ενημερώσει τον πυρήνα GENERIC στο /boot/GENERIC (αν υπάρχει), ακόμα και αν δεν είναι ο ενεργός πυρήνας του συστήματος (αυτός που εκτελείται τη συγκεκριμένη στιγμή).

Είναι γενικά καλή ιδέα να έχετε πάντα ένα αντίγραφο του πυρήνα GENERIC στον κατάλογο /boot/GENERIC. Θα σας βοηθήσει στην διάγνωση διάφορων προβλημάτων, καθώς και στην αναβάθμιση σε επόμενες εκδόσεις του FreeBSD, μέσω του `freebsd-update`. Η διαδικασία αυτή περιγράφεται στο Αναβαθμίσεις σε Μικρές και Μεγάλες Εκδόσεις.

Αν δεν έχουν γίνει αλλαγές στις προεπιλεγμένες ρυθμίσεις στο αρχείο /etc/freebsd-update.conf, το `freebsd-update` θα εγκαταστήσει τα ανανεωμένα αρχεία πηγαίου κώδικα μαζί με τις υπόλοιπες ενημερώσεις. Μπορείτε έπειτα να προχωρήσετε στη μεταγλώττιση και εγκατάσταση νέου προσαρμοσμένου πυρήνα, με το συνήθη τρόπο.

Οι ενημερώσεις που διανέμονται μέσω του `freebsd-update` δεν περιλαμβάνουν πάντοτε αλλαγές στον πυρήνα. Δεν είναι απαραίτητο να επαναμεταγλωττίσετε τον προσαρμοσμένο πυρήνα σας, αν η εκτέλεση του `freebsd-update install` δεν επέφερε αλλαγές στα αρχεία πηγαίου κώδικα του πυρήνα. Ωστόσο, το `freebsd-update` ενημερώνει πάντοτε το αρχείο /usr/src/sys/conf/newvers.sh. Το αρχείο αυτό περιέχει το τρέχον επίπεδο ενημερώσεων (patch level) το οποίο και αναφέρεται ως αριθμός `-p` από εντολές όπως η `uname -r`. Μεταγλωττίζοντας ξανά τον προσαρμοσμένο πυρήνα σας (ακόμα και αν δεν υπάρχουν άλλες αλλαγές) θα δώσετε τη δυνατότητα στην uname(1) να αναφέρει με ακρίβεια το επίπεδο ενημερώσεων. Αυτό μπορεί να είναι ιδιαίτερα χρήσιμο όταν συντηρείτε πολλαπλά συστήματα, καθώς σας επιτρέπει να αξιολογήσετε με μια ματιά τι ενημερώσεις έχουν εγκατασταθεί στο καθένα.

44.2.3. Αναβαθμίσεις σε Μικρές και Μεγάλες Εκδόσεις

Η διαδικασία αυτή θα απομακρύνει τα παλιά αρχεία αντικειμενικού κώδικα (object files) καθώς και τις παλιές βιβλιοθήκες, κάνοντας τις περισσότερες εφαρμογές τρίτων κατασκευαστών να μη λειτουργούν. Σας συνιστούμε είτε να απεγκαταστήσετε όλα τα εγκατεστημένα ports και να τα εγκαταστήσετε ξανά, ή να τα αναβαθμίσετε αργότερα, χρησιμοποιώντας το βοηθητικό πρόγραμμα ports-mgmt/portupgrade. Οι περισσότεροι χρήστες θα θέλουν να κάνουν μια δοκιμαστική μεταγλώττιση χρησιμοποιώντας την ακόλουθη εντολή:

```
# portupgrade -af
```

Με αυτό τον τρόπο εξασφαλίζεται ότι τα πάντα θα επανεγκατασταθούν σωστά. Σημειώστε ότι αν θέσετε την μεταβλητή περιβάλλοντος `BATCH` στην τιμή `yes`, όλες οι πιθανές ερωτήσεις που θα εμφανιστούν κατά τη διαδικασία, θα απαντηθούν αυτόματα με `yes`. Έτσι δεν υπάρχει πλέον ανάγκη για παρέμβαση του χρήστη κατά τη διάρκεια της διαδικασίας μεταγλώττισης.

Αν χρησιμοποιείται προσαρμοσμένος πυρήνας, η διαδικασία αναβάθμισης είναι ελαφρά πιο πολύπλοκη. Θα χρειαστείτε ένα αντίγραφο του πυρήνα GENERIC στον κατάλογο /boot/GENERIC. Αν δεν υπάρχει ήδη ο πυρήνας GENERIC στο σύστημα σας, μπορείτε να τον ανακτήσετε χρησιμοποιώντας μια από τις παρακάτω μεθόδους:

- Αν έχετε μεταγλωττίσει προσαρμοσμένο πυρήνα μόνο μια φορά, ο πυρήνας στον κατάλογο /boot/kernel.old είναι στην πραγματικότητα ο GENERIC. Απλώς μετονομάστε τον κατάλογο σε

/boot/GENERIC.

- Αν έχετε φυσική πρόσβαση στο μηχάνημα, μπορείτε να εγκαταστήσετε ένα αντίγραφο του πυρήνα GENERIC από το CD-ROM της εγκατάστασης. Τοποθετήστε το CD-ROM στον οδηγό και χρησιμοποιήστε τις παρακάτω εντολές:

  ```
  # mount /cdrom
  # cd /cdrom/X.Y-RELEASE/kernels
  # ./install.sh GENERIC
  ```

  Αντικαταστήστε το X.Y-RELEASE με τους πραγματικούς αριθμούς της έκδοσης που χρησιμοποιείτε. Ο πυρήνας GENERIC θα εγκατασταθεί από προεπιλογή στον κατάλογο /boot/GENERIC.

- Αν δεν έχετε κάποια από τις παραπάνω επιλογές, μπορείτε να μεταγλωττίσετε και να εγκαταστήσετε τον πυρήνα GENERIC μέσω του πηγαίου κώδικα:

  ```
  # cd /usr/src/
  # env DESTDIR=/boot/GENERIC make kernel
  # mv /boot/GENERIC/boot/kernel/* /boot/GENERIC
  # rm -rf /boot/GENERIC/boot
  ```

  Για να αναγνωριστεί αυτός ο πυρήνας ως GENERIC από το `freebsd-update`, δεν θα πρέπει να έχουν γίνει αλλαγές στο αρχείο ρυθμίσεων του GENERIC. Συνίσταται επίσης η μεταγλώττιση να γίνει χωρίς άλλες εξειδικευμένες ρυθμίσεις (κατά προτίμηση με κενό το /etc/make.conf).

Δεν χρειάζεται τη δεδομένη στιγμή να επανεκκινήσετε με τον πυρήνα GENERIC.

Είναι δυνατές οι αναβαθμίσεις τόσο σε μικρές όσο και σε μεγάλες εκδόσεις, δίνοντας στην εντολή `freebsd-update` τον επιθυμητό αριθμό έκδοσης. Για παράδειγμα, η ακόλουθη εντολή θα αναβαθμίσει το σύστημα σε FreeBSD 8.1:

```
# freebsd-update -r 8.1-RELEASE upgrade
```

Μετά τη λήψη της εντολής, το `freebsd-update` θα αξιολογήσει την κατάσταση του συστήματος και του αρχείου ρυθμίσεων του, σε μια απόπειρα να μαζέψει τις απαραίτητες πληροφορίες για την αναβάθμιση του συστήματος. Οι πληροφορίες που ανιχνεύθηκαν θα εμφανιστούν στην οθόνη με τη μορφή μιας λίστας εγκατεστημένων προγραμμάτων. Για παράδειγμα:

```
Looking up update.FreeBSD.org mirrors... 1 mirrors found.
Fetching metadata signature for 8.0-RELEASE from update1.FreeBSD.org... done.
Fetching metadata index... done.
Inspecting system... done.

The following components of FreeBSD seem to be installed:
kernel/smp src/base src/bin src/contrib src/crypto src/etc src/games
src/gnu src/include src/krb5 src/lib src/libexec src/release src/rescue
```

```
src/sbin src/secure src/share src/sys src/tools src/ubin src/usbin
world/base world/info world/lib32 world/manpages

The following components of FreeBSD do not seem to be installed:
kernel/generic world/catpages world/dict world/doc world/games
world/proflibs

Does this look reasonable (y/n)? y
```

Στο σημείο αυτό, το `freebsd-update` θα κατεβάσει όλα τα αρχεία που απαιτούνται για την αναβάθμιση. Σε μερικές περιπτώσεις, ο χρήστης θα κληθεί να απαντήσει σε ερωτήσεις σχετικά με το τι θα εγκατασταθεί ή πως πρέπει να προχωρήσει η διαδικασία.

Όταν χρησιμοποιείται προσαρμοσμένος πυρήνας, το παραπάνω βήμα θα προκαλέσει την εμφάνιση της παρακάτω προειδοποίησης:

```
WARNING: This system is running a "MYKERNEL" kernel, which is not a
kernel configuration distributed as part of FreeBSD 8.0-RELEASE.
This kernel will not be updated: you MUST update the kernel manually
before running "/usr/sbin/freebsd-update install"
```

Μπορείτε να αγνοήσετε αυτή την προειδοποίηση. Θα χρησιμοποιήσουμε τον ενημερωμένο πυρήνα GENERIC ως ενδιάμεσο βήμα στη διαδικασία αναβάθμισης.

Αφού μεταφορτωθούν όλα τα patches στο τοπικό σύστημα, θα γίνει και η εφαρμογή τους. Η διαδικασία αυτή ίσως πάρει λίγο χρόνο, ανάλογα με την ταχύτητα και το φορτίο του μηχανήματος. Έπειτα θα γίνει η συγχώνευση των αρχείων ρυθμίσεων. Αυτό το μέρος της διαδικασίας απαιτεί παρέμβαση του χρήστη, καθώς σε κάποια αρχεία θα χρειαστεί η συγχώνευση να γίνει χειροκίνητα με τη βοήθεια κάποιου συντάκτη κειμένου. Ο χρήστης θα ενημερώνεται για το αποτέλεσμα κάθε επιτυχημένης συγχώνευσης καθώς εξελίσσεται η διαδικασία. Σε περίπτωση αποτυχημένης συγχώνευσης (ή αγνόησης της), η διαδικασία αναβάθμισης θα διακοπεί. Ενδεχομένως να θέλετε να κρατήσετε αντίγραφο ασφαλείας του καταλόγου /etc και να συγχωνεύσετε αργότερα (χειροκίνητα) κάποια σημαντικά αρχεία, όπως το master.passwd ή το group.

Στο σημείο αυτό δεν έχει γίνει ακόμα καμιά αλλαγή στο σύστημα, καθώς όλη η διαδικασία της αναβάθμισης και συγχώνευσης γίνεται σε διαφορετικό κατάλογο. Όταν εφαρμοστούν επιτυχώς όλα τα patches και ολοκληρωθεί με επιτυχία η διαδικασία της συγχώνευσης όλων των αρχείων ρύθμισης, ο χρήστης θα πρέπει να επιβεβαιώσει την τελική εγκατάσταση.

Με το τέλος αυτής τη διαδικασίας, η αναβάθμιση μπορεί να οριστικοποιηθεί στο δίσκο, με τη χρήση της ακόλουθης εντολής:

```
# freebsd-update install
```

Στην πρώτη φάση, θα αλλαχθεί ο πυρήνας και τα σχετικά αρθρώματα. Στο σημείο αυτό, θα πρέπει να γίνει επανεκκίνηση του μηχανήματος. Σε μηχάνημα με προσαρμοσμένο πυρήνα, χρησιμοποιήστε

την εντολή nextboot(8) ώστε να θέσετε τον πυρήνα για την επόμενη εκκίνηση στον /boot/GENERIC (ο οποίος έχει ήδη αναβαθμιστεί):

```
# nextboot -k GENERIC
```

Πριν επανεκκινήσετε με τον πυρήνα GENERIC, βεβαιωθείτε ότι περιέχει όλα τα προγράμματα οδήγησης που απαιτούνται για την επιτυχή εκκίνηση του συστήματος σας (και τη λειτουργία του δικτύου, αν αναβαθμίζετε κάποιο απομακρυσμένο μηχάνημα). Ειδικότερα, αν ο προηγούμενος προσαρμοσμένος πυρήνας περιείχε λειτουργίες που συνήθως παρέχονται από αρθρώματα (modules), βεβαιωθείτε ότι φροντίσατε να φορτωθούν προσωρινά στον πυρήνα GENERIC χρησιμοποιώντας τις δυνατότητες του αρχείου /boot/loader.conf. Ίσως επίσης να θέλετε να απενεργοποιήσετε υπηρεσίες, προσαρτήσεις δίσκων και δικτύου κ.λ.π. που δεν είναι απαραίτητες, μέχρι την ολοκλήρωση της διαδικασίας αναβάθμισης.

Μπορείτε να χρησιμοποιήσετε την ακόλουθη εντολή για να επανεκκινήσετε το μηχάνημα με τον νέο πυρήνα:

```
# shutdown -r now
```

Μόλις το σύστημα επανέλθει σε λειτουργία, θα πρέπει να εκτελέσετε ξανά το `freebsd-update`. Η προηγούμενη λειτουργία έχει αποθηκευθεί, και έτσι το `freebsd-update` δεν θα ξεκινήσει από την αρχή, αλλά θα απομακρύνει όλες τις παλιές κοινόχρηστες βιβλιοθήκες και τα αρχεία αντικειμενικού κώδικα. Για να συνεχίσετε σε αυτό το στάδιο, δώστε την ακόλουθη εντολή:

```
# freebsd-update install
```

Ανάλογα με το αν υπήρξαν αλλαγές στους αριθμούς εκδόσεων των βιβλιοθηκών, ίσως να υπάρχουν μόνο δύο φάσεις εγκατάστασης αντί για τρεις.

Όλο το λογισμικό τρίτου κατασκευαστή θα πρέπει τώρα να μεταγλωττιστεί και να επανεγκατασταθεί από την αρχή. Αυτό απαιτείται καθώς το εγκατεστημένο λογισμικό ίσως εξαρτάται από βιβλιοθήκες οι οποίες αφαιρέθηκαν κατά τη διαδικασία της αναβάθμισης. Μπορείτε να χρησιμοποιήσετε την εντολή ports-mgmt/portupgrade για να αυτοματοποιήσετε αυτή τη διαδικασία. Για να ξεκινήσετε, δώστε τις παρακάτω εντολές:

```
# portupgrade -f ruby
# rm /var/db/pkg/pkgdb.db
# portupgrade -f ruby18-bdb
# rm /var/db/pkg/pkgdb.db /usr/ports/INDEX-*.db
# portupgrade -af
```

Μόλις ολοκληρωθεί το παραπάνω, ολοκληρώστε τη διαδικασία αναβάθμισης με μια τελευταία κλήση της εντολής `freebsd-update`. Δώστε την παρακάτω εντολή για να ολοκληρώσετε οτιδήποτε έχει

απομείνει στη διαδικασία αναβάθμισης:

```
# freebsd-update install
```

Αν χρησιμοποιούσατε προσωρινά τον πυρήνα GENERIC, αυτή είναι η κατάλληλη στιγμή για να μεταγλωττίσετε και να εγκαταστήσετε νέο προσαρμοσμένο πυρήνα, με το συνήθη τρόπο.

Επανεκκινήστε το μηχάνημα σας στην νέα έκδοση του FreeBSD. Η διαδικασία έχει ολοκληρωθεί.

44.2.4. Σύγκριση Κατάστασης του Συστήματος

Το βοηθητικό πρόγραμμα `freebsd-update` μπορεί να χρησιμοποιηθεί για να ελέγξετε την κατάσταση της εγκατεστημένης έκδοσης του FreeBSD σε σχέση με μια γνωστή και σωστή εγκατάσταση. Η επιλογή αυτή συγκρίνει και αξιολογεί την τρέχουσα έκδοση των προγραμμάτων συστήματος, των βιβλιοθηκών και των αρχείων ρύθμισης. Για να ξεκινήσετε τη σύγκριση, δώστε την ακόλουθη εντολή:

```
# freebsd-update IDS >> outfile.ids
```

Αν και το όνομα της εντολής είναι IDS, δεν θα πρέπει σε καμιά περίπτωση να θεωρηθεί υποκατάστατο ενός συστήματος ανίχνευσης εισβολέα (intrusion detection system) όπως είναι για παράδειγμα το security/snort. Καθώς το `freebsd-update` αποθηκεύει τα δεδομένα του στο δίσκο, υπάρχει πάντα η πιθανότητα να έχει γίνει αλλοίωση τους. Αν και η πιθανότητα αυτή μπορεί να μειωθεί χρησιμοποιώντας τη ρύθμιση `kern.securelevel` και αποθηκεύοντας τα δεδομένα της εντολής `freebsd-update` σε ένα σύστημα αρχείων μόνο για ανάγνωση, μια ακόμα καλύτερη λύση θα ήταν να συγκρίνετε το σύστημα με κάποιο δίσκο που θεωρείτε σίγουρα ασφαλή. Μπορείτε να χρησιμοποιήσετε ένα δίσκο DVD ή ένα εξωτερικό δίσκο USB που φυλάσσετε σε ασφαλή τοποθεσία.

Θα γίνει τώρα μια επιθεώρηση του συστήματος και θα εκτυπωθεί μια λίστα από αρχεία και τιμές hash του τύπου sha256(1), τόσο για το εγκατεστημένο όσο και για το γνωστό σύστημα. Επειδή πρόκειται για μεγάλη λίστα, την ανακατευθύνουμε στο αρχείο outfile.ids. Στην οθόνη το κείμενο θα κυλούσε πολύ γρήγορα, και σύντομα θα γέμιζε την προσωρινή μνήμη απεικόνισης της κονσόλας.

Οι γραμμές αυτές έχουν γενικά μεγάλο μήκος, αλλά είναι εύκολο να επεξεργαστούμε την έξοδο. Για παράδειγμα, για να δείτε μια λίστα όλων των αρχείων που διαφέρουν από αυτά της επίσημης έκδοσης, δώστε την ακόλουθη εντολή:

```
# cat outfile.ids | awk '{ print $1 }' | more
/etc/master.passwd
/etc/motd
/etc/passwd
/etc/pf.conf
```

Τα παραπάνω είναι μόνο ένα μέρος της εξόδου, υπάρχουν ακόμα πολλά διαφορετικά αρχεία. Κάποια

από αυτά τα αρχεία είναι φυσιολογικό να έχουν τροποποιηθεί. Για παράδειγμα, το /etc/passwd έχει τροποποιηθεί, καθώς έχουν προστεθεί χρήστες στο σύστημα. Σε μερικές περιπτώσεις, μπορεί να υπάρχουν και άλλα αρχεία, όπως π.χ. αρθρώματα πυρήνα τα οποία διαφέρουν αφού έχουν ενημερωθεί μέσω της `freebsd-update`. Για να εξαιρέσετε συγκεκριμένα αρχεία ή καταλόγους, προσθέστε τα στην επιλογή `IDSIgnorePaths` στο αρχείο ρυθμίσεων /etc/freebsd-update.conf.

Εκτός από την χρήση που αναφέραμε προηγουμένως, το σύστημα αυτό μπορεί να χρησιμοποιηθεί και ως τμήμα μιας λεπτομερούς διαδικασίας αναβάθμισης.

44.3. Portsnap: Ένα Εργαλείο Ενημέρωσης της Συλλογής των Ports

Το βασικό σύστημα του FreeBSD περιλαμβάνει επίσης ένα βοηθητικό πρόγραμμα για την ενημέρωση της Συλλογής των Ports. Πρόκειται για το portsnap(8). Όταν το εκτελέσετε, θα συνδεθεί σε ένα απομακρυσμένο διακομιστή, θα επαληθεύσει το κλειδί του πηγαίου κώδικα, και θα κατεβάσει ένα νέο αντίγραφο της Συλλογής των Ports. Το κλειδί χρησιμοποιείται για να επαληθεύσει την ακεραιότητα όλων των αρχείων που μεταφορτώνονται, εξασφαλίζοντας ότι δεν έχουν αλλοιωθεί κατά την μεταφορά. Για να κατεβάσετε τα τελευταία αρχεία της Συλλογής των Ports, εκτελέστε την ακόλουθη εντολή:

```
# portsnap fetch
Looking up portsnap.FreeBSD.org mirrors... 9 mirrors found.
Fetching snapshot tag from geodns-1.FreeBSD.org... done.
Fetching snapshot metadata... done.
Updating from Tue May 22 02:12:15 CEST 2012 to Wed May 23 16:28:31 CEST 2012.
Fetching 3 metadata patches.. done.
Applying metadata patches... done.
Fetching 3 metadata files... done.
Fetching 90 patches.....10....20....30....40....50....60....70....80....90. done.
Applying patches... done.
Fetching 133 new ports or files... done.
```

Το παραπάνω παράδειγμα δείχνει ότι το portsnap(8) βρήκε και επαλήθευσε αρκετά patches τα οποία πρέπει να εφαρμοστούν στο υπάρχον δέντρο των ports. Αυτό δείχνει επίσης ότι το πρόγραμμα έχει εκτελεστεί κατά το παρελθόν. Αν αυτή ήταν η πρώτη φορά που εκτελούνταν, θα γίνονταν απλώς κατέβασμα της συλλογής.

Όταν το portsnap(8) εκτελέσει επιτυχώς τη λειτουργία `fetch`, η Συλλογή των Ports και τα αντίστοιχα patches έχουν αποθηκευθεί στο τοπικό σύστημα και έχει γίνει η επαλήθευση τους. Την πρώτη φορά που θα εκτελέσετε το `portsnap`, θα πρέπει να χρησιμοποιήσετε το `extract` για να εγκαταστήσετε τα ενημερωμένα αρχεία:

```
# portsnap extract
/usr/ports/.cvsignore
/usr/ports/CHANGES
/usr/ports/COPYRIGHT
/usr/ports/GIDs
```

```
/usr/ports/KNOBS
/usr/ports/LEGAL
/usr/ports/MOVED
/usr/ports/Makefile
/usr/ports/Mk/bsd.apache.mk
/usr/ports/Mk/bsd.autotools.mk
/usr/ports/Mk/bsd.cmake.mk
...
```

Αν έχετε ήδη εγκατεστημένη την Συλλογή των Ports, χρησιμοποιήστε την εντολή `portsnap update` για να την ενημέρωσετε:

```
# portsnap update
```

Η διαδικασία έχει πλέον ολοκληρωθεί, και μπορείτε να εγκαταστήσετε ή να αναβαθμίσετε εφαρμογές χρησιμοποιώντας την ενημερωμένη Συλλογή των Ports.

Μπορείτε να εκτελέσετε τις διαδικασίες `fetch` και `extract` ή `update` διαδοχικά, όπως φαίνεται στο παρακάτω παράδειγμα:

```
# portsnap fetch update
```

Η παραπάνω εντολή θα κατεβάσει την τελευταία έκδοση της Συλλογής των Ports και θα ενημερώσει τα τοπικά αρχεία σας στον κατάλογο /usr/ports.

44.4. Ενημερώνοντας την Τεκμηρίωση

Εκτός από το βασικό σύστημα και την Συλλογή των Ports, η τεκμηρίωση αποτελεί επίσης βασικό τμήμα ενός συστήματος FreeBSD. Αν και πάντα μπορείτε να βρείτε την πιο πρόσφατη τεκμηρίωση στην δικτυακή τοποθεσία του FreeBSD, ορισμένοι χρήστες ίσως έχουν αργή ή μη σταθερή σύνδεση με το Διαδίκτυο. Ευτυχώς υπάρχουν αρκετοί τρόποι για να ενημερώσετε την τεκμηρίωση η οποία παρέχεται με κάθε επίσημη έκδοση, διατηρώντας το δικό σας τοπικό αντίγραφο της πιο πρόσφατης τεκμηρίωσης του FreeBSD.

44.4.1. Χρησιμοποιώντας το CVSup για την Ενημέρωση της Τεκμηρίωσης

Ο πηγαίος κώδικας και το εγκατεστημένο αντίγραφο της τεκμηρίωσης του FreeBSD, μπορούν να ενημερωθούν με την βοήθεια του CVSup, χρησιμοποιώντας ένα μηχανισμό παρόμοιο με αυτόν που χρησιμοποιείται στο βασικό σύστημα (δείτε το Μεταγλωττίζοντας το Βασικό Σύστημα ("world")). Η ενότητα αυτή περιγράφει:

- Πως να εγκαταστήσετε τα εργαλεία που απαιτούνται για την τεκμηρίωση, με τα οποία μπορείτε να δημιουργήσετε την τεκμηρίωση του FreeBSD ξεκινώντας από τον πηγαίο της κώδικα.
- Πως να κατεβάσετε ένα αντίγραφο του πηγαίου κώδικα της τεκμηρίωσης στον κατάλογο /usr/doc χρησιμοποιώντας το CVSup.

- Πως να αναδημιουργήσετε την τεκμηρίωση του FreeBSD από τον πηγαίο της κώδικα, και να την εγκαταστήσετε στον κατάλογο /usr/shared/doc/.

44.4.2. Εγκαθιστώντας το CVSup και τη Σειρά Εργαλείων της Τεκμηρίωσης

Η αναδημιουργία της τεκμηρίωσης του FreeBSD από τον πηγαίο κώδικα, απαιτεί μια σχετικά μεγάλη συλλογή εργαλείων. Τα εργαλεία αυτά δεν είναι μέρος του βασικού συστήματος του FreeBSD, καθώς χρειάζονται αρκετό χώρο στο δίσκο και δεν είναι χρήσιμα σε όλους τους χρήστες. Είναι χρήσιμα μόνο στους χρήστες που ασχολούνται με τη συγγραφή νέας τεκμηρίωσης για το FreeBSD, ή που ενημερώνουν συχνά την τοπική τους τεκμηρίωση μέσω του πηγαίου κώδικα.

Όλα τα απαιτούμενα εργαλεία διατίθενται μέσω της Συλλογής των Ports. Το textproc/docproj είναι το κύριο port το οποίο έχει αναπτυχθεί από την Ομάδα Τεκμηρίωσης του FreeBSD, για να βοηθήσει στην αρχική εγκατάσταση και τις μελλοντικές αναβαθμίσεις αυτών των εργαλείων.

Αν δεν απαιτείται η δημιουργία τεκμηρίωσης σε μορφές PostScript® ή PDF, μπορείτε να εγκαταστήσετε το port textproc/docproj-nojadetex. Αυτή η έκδοση των εργαλείων περιέχει τα πάντα εκτός από την μηχανή στοιχειοθεσίας teTeX. Το teTeX είναι μια αρκετά μεγάλη συλλογή εργαλείων, και δεν έχει νόημα να το εγκαταστήσετε αν δεν σας είναι απαραίτητη η παραγωγή της τεκμηρίωσης σε μορφή PDF.

Για περισσότερες πληροφορίες σχετικά με την εγκατάσταση και χρήση του CVSup, δείτε την ενότητα Χρησιμοποιώντας το CVSup.

44.4.3. Ενημερώνοντας τον Πηγαίο Κώδικα της Τεκμηρίωσης

Το βοηθητικό πρόγραμμα CVSup μπορεί να κατεβάσει ένα καθαρό αντίγραφο του πηγαίου κώδικα της τεκμηρίωσης, χρησιμοποιώντας το /usr/shared/examples/cvsup/doc-supfile ως πρότυπο αρχείο ρυθμίσεων. Ο προεπιλεγμένος υπολογιστής ενημερώσεων στο παραπάνω αρχείο είναι ρυθμισμένος σε πλασματική τιμή. Ωστόσο, η cvsup(1) δέχεται όνομα υπολογιστή μέσω της γραμμής εντολών, έτσι μπορείτε να ανακτήσετε τον πηγαίο κώδικα της τεκμηρίωσης μέσω κάποιου εξυπηρετητή CVSup γράφοντας:

```
# cvsup -h cvsup.FreeBSD.org -g -L 2 /usr/shared/examples/cvsup/doc-supfile
```

Αλλάξτε το *cvsup.FreeBSD.org* με τον κοντινότερο σας εξυπηρετητή CVSup. Δείτε το Τοποθεσίες CVSup για μια πλήρη λίστα των mirror sites.

Το αρχικό κατέβασμα του πηγαίου κώδικα της τεκμηρίωσης μπορεί να διαρκέσει αρκετή ώρα. Αφήστε το να εκτελείται μέχρι να ολοκληρωθεί.

Μπορείτε να συνεχίσετε να ενημερώνετε τον πηγαίο κώδικα της τεκμηρίωσης χρησιμοποιώντας την ίδια εντολή. Το βοηθητικό πρόγραμμα CVSup κατεβάζει και αντιγράφει μόνο τις ενημερώσεις σε σχέση με την τελευταία εκτέλεση του, έτσι κάθε εκτέλεση του CVSup μετά την πρώτη θα πρέπει να είναι αρκετά γρήγορη.

Μετά την αρχική ανάκτηση του πηγαίου κώδικα, ένας εναλλακτικός τρόπος ενημέρωσης της

τεκμηρίωσης είναι μέσω του αρχείου Makefile στον κατάλογο /usr/doc. Θέτοντας τις μεταβλητές SUP_UPDATE, SUPHOST και DOCSUPFILE στο αρχείο /etc/make.conf, μπορείτε να εκτελέσετε:

```
# cd /usr/doc
# make update
```

Τυπικές τιμές για τις παραπάνω επιλογές του make(1) στο αρχείο /etc/make.conf είναι:

```
SUP_UPDATE= yes
SUPHOST?= cvsup.freebsd.org
DOCSUPFILE?= /usr/shared/examples/cvsup/doc-supfile
```

Αν θέσετε τις τιμές των SUPHOST και DOCSUPFILE σε ?=, θα μπορείτε να ορίσετε άλλες τιμές για αυτές στη γραμμή εντολής του make. Αυτός είναι και ο συνιστώμενος τρόπος να προσθέσετε επιλογές στο make.conf, ώστε να αποφεύγετε να τροποποιείτε συνέχεια το αρχείο κάθε φορά που θέλετε να δοκιμάσετε μια νέα τιμή σε μια επιλογή.

44.4.4. Προσαρμογή Επιλογών στον Πηγαίο Κώδικα της Τεκμηρίωσης

Το σύστημα ενημέρωσης και μεταγλώττισης της τεκμηρίωσης του FreeBSD, υποστηρίζει μερικές επιλογές που διευκολύνουν τη διαδικασία ενημέρωσης ενός μόνο μέρους της τεκμηρίωσης, ή την μεταγλώττιση της τεκμηρίωσης κάποιων συγκεκριμένων μεταφράσεων. Αν θέλετε οι επιλογές αυτές να ισχύουν μόνιμα, μπορείτε να τις ορίσετε μέσα στο αρχείο /etc/make.conf, διαφορετικά μπορείτε να τις ορίζετε κάθε φορά στη γραμμή εντολής της make(1).

Κάποιες από τις επιλογές αυτές φαίνονται παρακάτω:

DOC_LANG
: Λίστα των γλωσσών και κωδικοποιήσεων που θα μεταγλωττιστούν και θα εγκατασταθούν, π.χ. en_US.ISO8859-1 αν είναι επιθυμητή μόνο η Αγγλική τεκμηρίωση.

FORMATS
: Η μορφή (ή μια λίστα από μορφές) στην οποία θα παραχθεί η μεταγλωττισμένη τεκμηρίωση. Τη δεδομένη στιγμή υποστηρίζονται οι μορφές html, html-split, txt, ps, pdf και rtf.

SUPHOST
: Το όνομα του εξυπηρετητή CVSup που θα χρησιμοποιηθεί κατά την ενημέρωση.

DOCDIR
: Ο κατάλογος στον οποίο θα εγκατασταθεί η τεκμηρίωση. Από προεπιλογή είναι ο /usr/shared/doc.

Για περισσότερες πληροφορίες σχετικά με τις μεταβλητές του make που υποστηρίζονται ως επιλογές συστήματος στο FreeBSD, δείτε την σελίδα manual του make.conf(5).

Για περισσότερες πληροφορίες και μεταβλητές make που υποστηρίζονται από το σύστημα μεταγλώττισης της τεκμηρίωσης του FreeBSD, παρακαλούμε δείτε τις Οδηγίες της Ομάδας

Τεκμηρίωσης του FreeBSD για Νέους Συγγραφείς.

44.4.5. Εγκατάσταση της Τεκμηρίωσης του FreeBSD από τον Πηγαίο Κώδικα

Έχοντας ενημερώσει το τοπικό αντίγραφο του πηγαίου κώδικα της τεκμηρίωσης στον κατάλογο /usr/doc, είμαστε έτοιμοι για την ενημέρωση της εγκατεστημένης τεκμηρίωσης.

Μπορείτε να προχωρήσετε σε πλήρη ενημέρωση όλων των γλωσσών που ορίζονται στην επιλογή DOC_LANG του Makefile, γράφοντας:

```
# cd /usr/doc
# make install clean
```

Αν έχετε ρυθμίσει το make.conf με τις σωστές τιμές για τις επιλογές DOCSUPFILE, SUPHOST και SUP_UPDATE, μπορείτε να συνδυάσετε τα βήματα ενημέρωσης και εγκατάστασης του πηγαίου κώδικα σε ένα, γράφοντας:

```
# cd /usr/doc
# make update install clean
```

Αν επιθυμείτε την ενημέρωση μιας μόνο συγκεκριμένης γλώσσας, μπορείτε να καλέσετε την make(1) σε ένα συγκεκριμένο υποκατάλογο του /usr/doc, π.χ.:

```
# cd /usr/doc/en_US.ISO8859-1
# make update install clean
```

Μπορείτε να καθορίσετε τη μορφή της τεκμηρίωσης που θα εγκατασταθεί, ρυθμίζοντας τη μεταβλητή FORMATS του make, π.χ.:

```
# cd /usr/doc
# make FORMATS='html html-split' install clean
```

44.4.6. Χρησιμοποιώντας τα Ports της Τεκμηρίωσης

Στην προηγούμενη ενότητα, παρουσιάσαμε μια μέθοδο για την ενημέρωση της τεκμηρίωσης του FreeBSD μέσω του πηγαίου κώδικα. Ωστόσο, οι ενημερώσεις που βασίζονται στον πηγαίο κώδικα μπορεί να μην είναι δυνατές ή πρακτικές για κάθε σύστημα FreeBSD. Η διαδικασία μεταγλώττισης του πηγαίου κώδικα της τεκμηρίωσης απαιτεί σχετικά μεγάλο αριθμό εργαλείων και βοηθητικών προγραμμάτων, γνωστά ως *εργαλεία τεκμηρίωσης*. Απαιτεί επίσης και μια σχετική εξοικείωση με το CVS και τη διαδικασία ανάκτησης των αρχείων από αυτό, καθώς και μια σειρά από βήματα για τη μεταγλώττιση του κώδικα. Στην ενότητα αυτή περιγράφουμε ένα εναλλακτικό τρόπο ενημέρωσης της τεκμηρίωσης που εγκαθίσταται μαζί με το FreeBSD. Η μέθοδος αυτή χρησιμοποιεί την Συλλογή των Ports και δίνει τις παρακάτω δυνατότητες:

- Κατέβασμα και εγκατάσταση προ-μεταγλωττισμένων στιγμιότυπων της τεκμηρίωσης, χωρίς να

απαιτείται καμιά τοπική μεταγλώττιση (εξαλείφοντας έτσι και την ανάγκη εγκατάστασης όλων των εργαλείων τεκμηρίωσης).

- Κατέβασμα του πηγαίου κώδικα της τεκμηρίωσης και μεταγλώττιση του μέσω των δυνατοτήτων που παρέχουν τα εργαλεία των ports (απλοποιώντας με αυτό τον τρόπο τη χειροκίνητη διαδικασία ανάκτησης και μεταγλώττισης).

Αυτές οι δύο μέθοδοι ενημέρωσης της τεκμηρίωσης του FreeBSD υποστηρίζονται από μια σειρά από *ports τεκμηρίωσης* τα οποία ενημερώνονται κάθε μήνα από την Ομάδα Αρχιτεκτονικής της Τεκμηρίωσης <doceng@FreeBSD.org>. Στη Συλλογή των Ports, θα τα βρείτε κάτω από την κατηγορία docs.

44.4.6.1. Μεταγλώττιση και Εγκατάσταση των Ports της Τεκμηρίωσης

Τα ports της τεκμηρίωσης χρησιμοποιούν τις δυνατότητες μεταγλώττισης που παρέχει το σύστημα των ports ώστε να διευκολύνουν τη διαδικασία δημιουργίας της τεκμηρίωσης. Με αυτό τον τρόπο η ανάκτηση του πηγαίου κώδικα της τεκμηρίωσης γίνεται αυτόματα με την εκτέλεση της make(1) και τις κατάλληλες ρυθμίσεις στο περιβάλλον. Η εγκατάσταση και απεγκατάσταση της τεκμηρίωσης είναι το ίδιο εύκολη με την εγκατάσταση οποιουδήποτε άλλου port ή πακέτου στο FreeBSD.

Σε περίπτωση τοπικής μεταγλώττισης των ports της τεκμηρίωσης, απαιτείται και η εγκατάσταση των *εργαλείων τεκμηρίωσης*. Τα εργαλεία αυτά ωστόσο θα εγκατασταθούν αυτόματα.

Η οργάνωση των ports τεκμηρίωσης φαίνεται παρακάτω:

- Υπάρχει ένα κεντρικό "master port", το misc/freebsd-doc-en το οποίο διαθέτει τα απαραίτητα αρχεία και αποτελεί την βάση όλων των άλλων ports τεκμηρίωσης. Από προεπιλογή, το port αυτό μεταγλωττίζει μόνο την Αγγλική τεκμηρίωση.
- Υπάρχει ένα port "όλα σε ένα", το misc/freebsd-doc-all το οποίο μεταγλωττίζει και εγκαθιστά όλη την τεκμηρίωση σε όλες τις διαθέσιμες γλώσσες.
- Τέλος, υπάρχει ένα "εξαρτώμενο port" για κάθε μετάφραση, π.χ.: misc/freebsd-doc-el για την Ελληνική τεκμηρίωση. Όλα αυτά τα ports εξαρτώνται από το master port και εγκαθιστούν την τεκμηρίωση που έχει μεταφραστεί στην αντίστοιχη γλώσσα.

Για να εγκαταστήσετε ένα port τεκμηρίωσης από τον πηγαίο κώδικα, εκτελέστε τις παρακάτω εντολές (ως `root`):

```
# cd /usr/ports/misc/freebsd-doc-en
# make install clean
```

Το παραπάνω θα μεταγλωττίσει και θα εγκαταστήσει την Αγγλική τεκμηρίωση σε μορφή τμηματικών HTML κειμένων (όπως χρησιμοποιούνται και στο http://www.FreeBSD.org), στον κατάλογο /usr/local/shared/doc/freebsd.

44.4.6.1.1. Συνηθισμένες Επιλογές και Παράμετροι Μεταγλώττισης

Μπορείτε να χρησιμοποιήσετε αρκετές επιλογές για την τροποποίηση της προεπιλεγμένης

συμπεριφοράς των ports τεκμηρίωσης. Παρακάτω δείχνουμε μερικές μόνο από αυτές:

`WITH_HTML`

Επιτρέπει τη δημιουργία της τεκμηρίωσης σε μορφή HTML. Θα δημιουργηθεί ένα αρχείο HTML για κάθε κείμενο. Η μορφοποιημένη τεκμηρίωση θα αποθηκευθεί, ανάλογα με την περίπτωση, σε ένα αρχείο με όνομα article.html ή book.html. Θα γίνει επίσης και αποθήκευση των αντίστοιχων εικόνων.

`WITH_PDF`

Επιτρέπει τη δημιουργία εγγράφου σε μορφή Adobe® Portable Document Format (PDF) για χρήση με τον Adobe® Acrobat Reader®, το Ghostscript, ή άλλα προγράμματα προβολής εγγράφων PDF. Η μορφοποιημένη τεκμηρίωση θα αποθηκευθεί, ανάλογα με την περίπτωση, σε ένα αρχείο article.pdf ή book.pdf.

`DOCBASE`

Πρόκειται για την θέση στην οποία θα εγκατασταθεί η τεκμηρίωση. Από προεπιλογή, είναι ο κατάλογος /usr/local/shared/doc/freebsd.

Παρατηρήστε ότι ο προεπιλεγμένος κατάλογος διαφέρει από αυτόν που χρησιμοποιείται στη μέθοδο CVSup. Αυτό συμβαίνει επειδή γίνεται εγκατάσταση port, τα οποία από προεπιλογή χρησιμοποιούν τον κατάλογο /usr/local. Μπορείτε να παρακάμψετε αυτή την προεπιλογή, αλλάζοντας την τιμή της μεταβλητής `PREFIX`.

Παρακάτω θα βρείτε ένα σύντομο παράδειγμα σχετικό με τη χρήση των μεταβλητών για την εγκατάσταση της Αγγλικής τεκμηρίωσης σε μορφή PDF:

```
# cd /usr/ports/misc/freebsd-doc-en
# make -DWITH_PDF DOCBASE=share/doc/freebsd/en install clean
```

44.4.6.2. Χρήση Έτοιμων Πακέτων Τεκμηρίωσης

Η μεταγλώττιση των ports τεκμηρίωσης από τον πηγαίο κώδικα (όπως είδαμε στην προηγούμενη ενότητα), απαιτεί τοπική εγκατάσταση των αντίστοιχων εργαλείων τεκμηρίωσης και επάρκεια χώρου στο δίσκο για την διαδικασία. Όταν δεν διατίθενται οι απαραίτητοι πόροι για την εγκατάσταση των εργαλείων τεκμηρίωσης (ή επειδή η μεταγλώττιση από τα ports θα χρησιμοποιούσε πολύ χώρο), η εγκατάσταση μπορεί να γίνει μέσω έτοιμων πακέτων τεκμηρίωσης.

Η Ομάδα Αρχιτεκτονικής της Τεκμηρίωσης <doceng@FreeBSD.org> προετοιμάζει μηνιαία στιγμιότυπα πακέτων τεκμηρίωσης του FreeBSD. Τα έτοιμα αυτά πακέτα μπορούν να χρησιμοποιηθούν με την βοήθεια οποιουδήποτε εργαλείου διαχείρισης πακέτων που διατίθεται με το FreeBSD, όπως για παράδειγμα τα pkg_add(1), pkg_delete(1) κ.λ.π.

Όταν χρησιμοποιείτε έτοιμα πακέτα, η εγκατάσταση της τεκμηρίωσης της επιλεγμένης γλώσσας θα γίνεται σε όλες τις διαθέσιμες μορφές.

Για παράδειγμα, η παρακάτω εντολή θα εγκαταστήσει την τελευταία έκδοση του έτοιμου πακέτου

της Ελληνικής τεκμηρίωσης:

```
# pkg_add -r el-freebsd-doc
```

Τα πακέτα χρησιμοποιούν τη μορφή `lang-freebsd-doc` στο όνομα τους, η οποία διαφέρει από την αντίστοιχη μορφή του port. Το *lang* είναι η σύντομη μορφή της γλώσσας, π.χ. `el` για Ελληνικά ή `zh_cn` για Απλοποιημένα Κινέζικα.

44.4.6.3. Ενημερώνοντας τα Ports της Τεκμηρίωσης

Για να ενημερώσετε ένα ήδη εγκατεστημένο port τεκμηρίωσης, μπορείτε να χρησιμοποιήσετε οποιοδήποτε εργαλείο αναβάθμισης ports. Για παράδειγμα, η παρακάτω εντολή ενημερώνει την εγκατεστημένη Ελληνική τεκμηρίωση μέσω του εργαλείου ports-mgmt/portupgrade με τη χρήση μόνο έτοιμων πακέτων:

```
# portupgrade -PP el-freebsd-doc
```

44.5. Παρακολούθηση Ενός Κλάδου Ανάπτυξης

Υπάρχουν δύο κλάδοι ανάπτυξης στο FreeBSD, το FreeBSD-CURRENT και το FreeBSD-STABLE. Στην ενότητα αυτή, θα εξηγήσουμε κάποια πράγματα σχετικά με αυτούς τους κλάδους, και θα περιγράψουμε πως μπορείτε να διατηρήσετε το σύστημα σας ενημερωμένο σε κάποιον από αυτούς. Θα μιλήσουμε αρχικά για το FreeBSD-CURRENT και έπειτα για το FreeBSD-STABLE.

44.5.1. Παρακολουθώντας το FreeBSD-CURRENT

Καθώς διαβάζετε αυτό το κείμενο, να έχετε υπόψιν σας ότι το FreeBSD-CURRENT είναι πράγματι η "κόψη του ξυραφιού" στην ανάπτυξη του FreeBSD. Οι χρήστες του FreeBSD-CURRENT αναμένεται να έχουν αυξημένες τεχνικές γνώσεις, και να είναι ικανοί να επιλύουν δύσκολα προβλήματα του συστήματος τους, χωρίς βοήθεια. Αν είστε καινούριος στο FreeBSD, μάλλον θα πρέπει να το ξανασκεφτείτε πριν το εγκαταστήσετε.

44.5.1.1. Τι Είναι το FreeBSD-CURRENT;

Το FreeBSD-CURRENT αποτελείται από τον πλέον πρόσφατο λειτουργικό πηγαίο κώδικα του FreeBSD. Περιλαμβάνει αλλαγές που βρίσκονται σε εξέλιξη, πειραματικές αλλαγές, και μηχανισμούς μετάβασης οι οποίοι δεν είναι σίγουρο ότι θα περιλαμβάνονται στην επόμενη επίσημη έκδοση του λογισμικού. Αν και πολλά μέλη της ομάδας ανάπτυξης του FreeBSD μεταγλωττίζουν καθημερινά τον πηγαίο κώδικα του FreeBSD-CURRENT, υπάρχουν χρονικές περίοδοι που η μεταγλώττιση του είναι αδύνατη. Τα προβλήματα αυτά γενικά επιλύονται όσο πιο γρήγορα γίνεται, αλλά το αν το FreeBSD-CURRENT θα σας φέρει την καταστροφή ή κάποιο πολυπόθητο χαρακτηριστικό, είναι περισσότερο θέμα της χρονικής στιγμής που θα επιλέξετε να ανακτήσετε τον πηγαίο κώδικα!

44.5.1.2. Ποιος Χρειάζεται το FreeBSD-CURRENT;

Το FreeBSD-CURRENT διατίθεται και ενδιαφέρει κυρίως τις παρακάτω τρεις ομάδες:

1. Μέλη της κοινότητας του FreeBSD που δουλεύουν ενεργά σε κάποιο τμήμα του πηγαίου κώδικα, και για τους οποίους η παρακολούθηση του FreeBSD-CURRENT είναι απόλυτα απαραίτητη.
2. Μέλη της κοινότητας του FreeBSD που είναι ενεργοί testers και είναι πρόθυμοι να αναλώσουν το χρόνο τους για να λύσουν προβλήματα, ώστε να εξασφαλίσουν ότι το FreeBSD-CURRENT θα παραμείνει όσο το δυνατόν πιο σωστό. Συνήθως, τα μέλη αυτά κάνουν προτάσεις για τοπικές αλλαγές και για την γενική κατεύθυνση του FreeBSD, και στέλνουν patches για την πραγματοποίηση τους.
3. Αυτοί που απλώς θέλουν να βλέπουν τις τελευταίες ενημερώσεις, ή να χρησιμοποιούν τον τελευταίο πηγαίο κώδικα ως αναφορά (π.χ. για *μελέτη* και όχι για εκτέλεση). Μέλη αυτής της ομάδας μπορεί επίσης περιστασιακά να συνεισφέρουν σχόλια ή κώδικα.

44.5.1.3. Τι *Δεν* Είναι το FreeBSD-CURRENT;

1. Δεν είναι ένας γρήγορος τρόπος να πάρετε κώδικα ο οποίος δεν έχει κυκλοφορήσει ακόμα σε κάποια έκδοση, με την ελπίδα ότι περιέχει κάποια νέα εκπληκτική δυνατότητα και θέλετε να είστε ο πρώτος που τη χρησιμοποιεί. Αν είστε πράγματι ο πρώτος που την χρησιμοποιεί, θα είστε επίσης και ο πρώτος που θα συναντήσετε τα νέα προβλήματα και bugs.
2. Δεν είναι ένας γρήγορος τρόπος για να ανακτήσετε διορθώσεις προβλημάτων. Κάθε νέα έκδοση του FreeBSD-CURRENT μπορεί να εισάγει τόσα νέα bugs όσα και αυτά που διορθώνει.
3. Το FreeBSD-CURRENT δεν αποτελεί "επίσημα υποστηριζόμενο" κώδικα. Αν και καταβάλλουμε κάθε δυνατή προσπάθεια να βοηθήσουμε όσους ανήκουν "πραγματικά" σε κάποια από τις τρεις ομάδες που αναφέραμε, ωστόσο *δεν έχουμε το χρόνο* να παρέχουμε τεχνική υποστήριξη. Αυτό δεν συμβαίνει επειδή είμαστε κακοήθεις και δύσκολοι και δεν θέλουμε να βοηθάμε τους ανθρώπους (δεν θα είχαμε καν δημιουργήσει το FreeBSD αν σκεφτόμασταν έτσι). Πολύ απλά, δεν μπορούμε να απαντάμε εκατοντάδες μηνύματα την ημέρα και *ταυτόχρονα* να δουλεύουμε στο FreeBSD! Αν δώσετε σε οποιοδήποτε μέλος της ομάδας ανάπτυξης την επιλογή να απαντάει σε πολλές ερωτήσεις σχετικά με πειραματικό κώδικα ή να δουλεύει για τη βελτίωση του FreeBSD, θα επιλέξει σίγουρα το δεύτερο.

44.5.1.4. Χρησιμοποιώντας το FreeBSD-CURRENT

1. Γραφτείτε στις λίστες ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT και ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα για τον κλάδο head/-current. Δεν είναι απλώς καλή ιδέα, είναι *βασικό* να το κάνετε. Αν δεν είστε γραμμένος στη λίστα *ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT*, δεν θα βλέπετε τα σχόλια σχετικά με την τρέχουσα κατάσταση του συστήματος από όσους το χρησιμοποιούν, και έτσι πιθανώς θα καταλήξετε να αντιμετωπίζετε πολλά προβλήματα που άλλοι έχουν ήδη ανακαλύψει και λύσει. Ακόμα πιο σημαντικό είναι ότι θα χάνετε σημαντικές ανακοινώσεις, οι οποίες μπορεί να είναι κρίσιμες για την διατήρηση του συστήματος σας σε υγιή κατάσταση.

   Η λίστα ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα για τον κλάδο head/-current θα σας επιτρέψει να βλέπετε τις καταχωρήσεις στο commit log για κάθε αλλαγή που γίνεται, καθώς και πληροφορίες για πιθανές παρενέργειες που μπορεί να έχει.

   Για να γραφτείτε σε αυτές, ή σε οποιεσδήποτε από τις υπάρχουσες λίστες, επισκεφθείτε την τοποθεσία https://lists.freebsd.org και επιλέξτε τη λίστα στην οποία θέλετε να γίνετε συνδρομητής. Οδηγίες για την υπόλοιπη διαδικασία θα βρείτε επιτόπου. Αν σας ενδιαφέρει να

παρακολουθείτε τις αλλαγές σε όλο το δέντρο πηγαίου κώδικα, σας συνιστούμε να εγγραφείτε στη λίστα ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα του FreeBSD (εξαιρούνται τα δέντρα "user" και "projects").

2. Ανακτήστε τον πηγαίο κώδικα από ένα mirror site του FreeBSD. Αυτό μπορεί να γίνει με δύο τρόπους:

   a. Χρησιμοποιήστε το πρόγραμμα cvsup σε συνδυασμό με το supfile με την ονομασία standard-supfile το οποίο θα βρείτε στον κατάλογο /usr/shared/examples/cvsup. Αυτή είναι και η πλέον συνιστώμενη μέθοδος, καθώς σας επιτρέπει να ανακτήσετε όλη τη συλλογή με μια κίνηση, και στις επόμενες ανανεώσεις θα παίρνετε μόνο τις αλλαγές. Πολλοί χρήστες εκτελούν το `cvsup` μέσω του `cron` ώστε να κρατάνε τον πηγαίο κώδικα του συστήματος τους πάντα ανανεωμένο αυτόματα. Θα πρέπει να προσαρμόσετε το υπόδειγμα του supfile που δίνουμε παραπάνω, και να ρυθμίσετε το cvsup για το περιβάλλον σας.

Το υπόδειγμα του αρχείου standard-supfile προορίζεται για χρήση με κάποιο συγκεκριμένο κλάδο ασφάλειας (security branch) του FreeBSD, και όχι με το FreeBSD-CURRENT. Θα πρέπει να επεξεργαστείτε το αρχείο και να αντικαταστήσετε την παρακάτω γραμμή:

```
*default release=cvs tag=RELENG_X_Y
```

με την ακόλουθη:

```
*default release=cvs tag=.
```

Για περισσότερες πληροφορίες σχετικά με τα tags που μπορείτε να χρησιμοποιήσετε, παρακαλούμε διαβάστε στο Εγχειρίδιο την ενότητα Ετικέτες (Tags) για το CVS.

   b. Χρησιμοποιήστε την υπηρεσία CTM. Αν έχετε πολύ κακή συνδεσιμότητα (υψηλό κόστος σύνδεσης ή πρόσβαση μόνο μέσω email) το CTM αποτελεί για σας μια εναλλακτική λύση. Μπορεί ωστόσο να σας δημιουργήσει διάφορα προβλήματα και να καταλήξετε με χαλασμένα αρχεία. Για το λόγο αυτό, το CTM χρησιμοποιείται σπάνια, κάτι το οποίο αυξάνει ακόμα περισσότερο την πιθανότητα να μη δουλεύει σωστά για μεγάλα χρονικά διαστήματα. Σας συνιστούμε να χρησιμοποιήσετε το CVSup αν διαθέτετε modem 9600 bps ή ταχύτερο.

3. Αν σκοπεύετε να ανακτήσετε τον πηγαίο κώδικα για κανονική χρήση (εκτέλεση) και όχι απλώς για να τον δείτε, τότε ανακτήστε *ολόκληρο* το FreeBSD-CURRENT και όχι κάποια επιλεγμένα τμήματα. Σε διαφορετική περίπτωση, είναι αρκετά πιθανό να συναντήσετε προβλήματα, καθώς πολλά κομμάτια του κώδικα εξαρτώνται από ανανεώσεις σε άλλα, και δεν μπορούν να μεταγλωττιστούν αυτόνομα.

   Πριν μεταγλωττίσετε το FreeBSD-CURRENT, διαβάστε προσεκτικά το Makefile στον κατάλογο /usr/src. Θα πρέπει να μεταγλωττίσετε τον πυρήνα και όλο το βασικό σύστημα (world) την πρώτη φορά, ως μέρος της διαδικασίας αναβάθμισης. Διαβάζοντας την ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT και το /usr/src/UPDATING θα είστε ενημερωμένοι για νέες διαδικασίες όσο αφορά την εκκίνηση στο νέο σας σύστημα. Οι διαδικασίες αυτές είναι συχνά

απαραίτητες όσο πλησιάζουμε σε μια νέα επίσημη έκδοση.

4. Γίνετε ενεργό μέλος! Αν χρησιμοποιείτε το FreeBSD-CURRENT, θέλουμε να ξέρουμε τη γνώμη σας για αυτό, ειδικά αν έχετε προτάσεις για βελτιώσεις ή διορθώσεις λαθών. Προτάσεις που συνοδεύονται και από κώδικα γίνονται δεκτές με ενθουσιασμό!

44.5.2. Χρησιμοποιώντας το FreeBSD-STABLE

44.5.2.1. Τι Είναι το FreeBSD-STABLE;

Το FreeBSD-STABLE είναι ένας κλάδος ανάπτυξης από τον οποίο προκύπτουν οι "μεγάλες" (major) εκδόσεις. Οι αλλαγές εισάγονται σε αυτό τον κλάδο με διαφορετικό ρυθμό, και με τη γενική παραδοχή ότι έχουν πρώτα περάσει από το FreeBSD-CURRENT για δοκιμή. Ωστόσο, *δεν παύει* να είναι ένας κλάδος ανάπτυξης, και αυτό σημαίνει ότι ο κώδικας του FreeBSD-STABLE μπορεί μια δεδομένη χρονική στιγμή να είναι ακατάλληλος για συγκεκριμένες εφαρμογές. Πρόκειται για μια ακόμα γραμμή ανάπτυξης για τους προγραμματιστές, και δεν είναι απαραίτητα κατάλληλη για τους τελικούς χρήστες.

44.5.2.2. Ποιος Χρειάζεται το FreeBSD-STABLE;

Αν σας ενδιαφέρει να παρακολουθείτε ή να συμβάλλετε στην ανάπτυξη του FreeBSD, και ειδικά όσο αφορά την επόμενη επίσημη έκδοση του από τον ίδιο κλάδο (point release), είναι καλή ιδέα να παρακολουθείτε το FreeBSD-STABLE.

Αν και είναι αλήθεια ότι οι διορθώσεις ασφάλειας γίνονται και στον κλάδο FreeBSD-STABLE, ωστόσο *δεν χρειάζεται* να παρακολουθείτε το FreeBSD-STABLE μόνο για αυτό το λόγο. Κάθε αναφορά προβλήματος ασφάλειας του FreeBSD εξηγεί πως να διορθώσετε το πρόβλημα για κάθε επίσημη έκδοση η οποία επηρεάζεται από αυτό , και η παρακολούθηση ενός κλάδου ανάπτυξης μόνο για λόγους ασφαλείας, πιθανόν να φέρει επίσης και άλλες ανεπιθύμητες αλλαγές μαζί της.

Αν και καταβάλλουμε κάθε δυνατή προσπάθεια ώστε να εξασφαλίσουμε ότι ο κλάδος FreeBSD-STABLE μπορεί να μεταγλωττιστεί και να εκτελεστεί σε κάθε δεδομένη χρονική στιγμή, δεν μπορούμε ωστόσο να το εγγυηθούμε. Επιπρόσθετα, αν και ο κώδικας αναπτύσσεται στο FreeBSD-CURRENT πριν περάσει στο FreeBSD-STABLE, ο κόσμος που εκτελεί το FreeBSD-STABLE είναι περισσότερος, και έτσι είναι αναπόφευκτο να ανακαλύπτονται πιο πολλά σφάλματα και ακραίες περιπτώσεις στο FreeBSD-STABLE τα οποία δεν έχουν γίνει εμφανή στο FreeBSD-CURRENT.

Για τους λόγους αυτούς, *δεν* συνιστούμε να παρακολουθείτε τυφλά το FreeBSD-STABLE, και ειδικότερα είναι σημαντικό να μην αναβαθμίζετε σε αυτό εξυπηρετητές σε περιβάλλοντα παραγωγής, χωρίς να έχετε πρώτα ελέγξει αναλυτικά τον κώδικα στο δικό σας περιβάλλον ανάπτυξης.

Αν δεν διαθέτετε τους πόρους για να το κάνετε αυτό, σας συνιστούμε να χρησιμοποιείτε την τελευταία επίσημη έκδοση του FreeBSD, και να αναβαθμίζεστε από τη μια έκδοση στην επόμενη μέσω του μηχανισμού δυαδικών ενημερώσεων.

44.5.2.3. Χρησιμοποιώντας το FreeBSD-STABLE

1. Γραφτείτε συνδρομητής στη λίστα ηλεκτρονική λίστα του FreeBSD-STABLE;. Θα είστε έτσι ενημερωμένοι για εξαρτήσεις μεταγλώττισης που ίσως εμφανιστούν στο FreeBSD-STABLE, ή για

άλλα προβλήματα που χρήζουν ειδικής προσοχής. Στη λίστα αυτή θα βρίσκετε επίσης ανακοινώσεις από μέλη της ομάδας ανάπτυξης, όταν πρόκειται να συμπεριληφθεί κάποια αμφιλεγόμενη ανανέωση ή διόρθωση, δίνοντας έτσι στους χρήστες την ευκαιρία να εκφέρουν γνώμη σχετικά με τα προβλήματα που θα προκαλέσει η προτεινόμενη αλλαγή.

Θα πρέπει να εγγραφείτε στην κατάλληλη λίστα SVN ανάλογα με τον κλάδο που παρακολουθείτε. Για παράδειγμα, αν παρακολουθείτε τον κλάδο 7-STABLE, η κατάλληλη λίστα είναι η svn-src-stable-7. Αυτό θα σας επιτρέψει να βλέπετε τις καταχωρήσεις στο commit log για κάθε αλλαγή που γίνεται, καθώς και πληροφορίες για πιθανές παρενέργειες που μπορεί να έχει.

Για να γραφτείτε σε αυτές, ή σε οποιεσδήποτε από τις υπάρχουσες λίστες, επισκεφθείτε την τοποθεσία https://lists.freebsd.org και επιλέξτε τη λίστα στην οποία θέλετε να γίνετε συνδρομητής. Οδηγίες για την υπόλοιπη διαδικασία θα βρείτε επιτόπου. Αν σας ενδιαφέρει να παρακολουθείτε τις αλλαγές σε όλο το δέντρο πηγαίου κώδικα, σας συνιστούμε να εγγραφείτε στη λίστα ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα του FreeBSD (εξαιρούνται τα δέντρα "user" και "projects").

2. Αν πρόκειται να εγκαταστήσετε ένα νέο σύστημα με σκοπό να εκτελείτε τα μηνιαία snapshot του FreeBSD-STABLE, παρακαλούμε να ελέγξετε την τοποθεσία Snapshots για περισσότερες πληροφορίες. Εναλλακτικά, είναι δυνατόν να εγκαταστήσετε το πιο πρόσφατο FreeBSD-STABLE από κάποιο mirror site ακολουθώντας τις παρακάτω οδηγίες ώστε να αναβαθμίσετε το σύστημα σας στην πλέον πρόσφατη έκδοση πηγαίου κώδικα του FreeBSD-STABLE.

   Αν διαθέτετε ήδη κάποια προηγούμενη έκδοση του FreeBSD και επιθυμείτε να αναβαθμιστείτε μέσω του πηγαίου κώδικα, μπορείτε εύκολα να χρησιμοποιήσετε κάποιο mirror site του FreeBSD. Υπάρχουν δύο τρόποι για να γίνει αυτό: .. Χρησιμοποιήστε το πρόγραμμα cvsup σε συνδυασμό με το supfile με την ονομασία stable-supfile το οποίο θα βρείτε στον κατάλογο /usr/shared/examples/cvsup. Αυτή είναι και η πλέον συνιστώμενη μέθοδος, καθώς σας επιτρέπει να ανακτήσετε όλη τη συλλογή με μια κίνηση, και στις επόμενες ανανεώσεις θα παίρνετε μόνο τις αλλαγές. Πολλοί χρήστες εκτελούν το `cvsup` μέσω του `cron` ώστε να κρατάνε τον πηγαίο κώδικα του συστήματος τους πάντα ανανεωμένο αυτόματα. Θα πρέπει να προσαρμόσετε το υπόδειγμα του supfile που δίνουμε παραπάνω, και να ρυθμίσετε το cvsup για το περιβάλλον σας. .. Χρησιμοποιήστε την υπηρεσία CTM. Αν δεν έχετε γρήγορη και φτηνή σύνδεση με το Internet, αυτή είναι η συνιστώμενη μέθοδος.

3. Ουσιαστικά, αν χρειάζεστε γρήγορη και κατά απαίτηση πρόσβαση στον πηγαίο κώδικα, και το εύρος ζώνης της σύνδεσης δεν αποτελεί πρόβλημα, χρησιμοποιήστε το `cvsup` ή το `ftp`. Διαφορετικά, χρησιμοποιήστε το CTM.

4. Πριν μεταγλωττίσετε το FreeBSD-STABLE, διαβάστε προσεκτικά το Makefile στον κατάλογο /usr/src. Θα πρέπει να μεταγλωττίσετε τον πυρήνα και όλο το βασικό σύστημα (world) την πρώτη φορά, ως μέρος της διαδικασίας αναβάθμισης. Διαβάζοντας την ηλεκτρονική λίστα του FreeBSD-STABLE; και το /usr/src/UPDATING θα είστε ενημερωμένοι για νέες διαδικασίες όσο αφορά την εκκίνηση στο νέο σας σύστημα. Οι διαδικασίες αυτές είναι συχνά απαραίτητες όσο πλησιάζουμε σε μια νέα επίσημη έκδοση.

44.6. Συγχρονίζοντας τον Πηγαίο σας Κώδικα

Υπάρχουν διάφοροι τρόποι να χρησιμοποιήσετε μια σύνδεση Internet (ή email) για να ενημερώνετε

οποιοδήποτε τμήμα πηγαίου κώδικα του FreeBSD Project σας ενδιαφέρει, ή και όλα αν το επιθυμείτε. Οι βασικές υπηρεσίες που προσφέρουμε είναι το Ανώνυμο CVS, το CVSup, και το CTM.

Αν και είναι δυνατόν να ενημερώσετε μόνο κάποια τμήματα του δέντρου πηγαίου κώδικα, η μόνη διαδικασία ενημέρωσης που υποστηρίζεται αφορά την ενημέρωση ολόκληρου του δέντρου. Μετά την ενημέρωση, θα πρέπει να μεταγλωττίσετε ξανά τόσο το userland (δηλ. τα προγράμματα που εκτελούνται στην περιοχή χρήστη, όπως αυτά που βρίσκονται στους καταλόγους /bin και /sbin) όσο και τον πηγαίο κώδικα του πυρήνα. Αν ενημερώσετε μόνο ένα τμήμα του πηγαίου κώδικα, μόνο τον πυρήνα ή μόνο το userland, θα αντιμετωπίσετε προβλήματα. Τα προβλήματα αυτά μπορεί να κυμαίνονται από σφάλματα μεταγλώττισης μέχρι kernel panic και καταστροφή δεδομένων.

Το Ανώνυμο CVS και το CVSup χρησιμοποιούν τη μέθοδο *pull* για την ενημέρωση του πηγαίου κώδικα. Στην περίπτωση του CVSup, ο χρήστης (η κάποιο script που εκτελείται μέσω `cron`) εκτελεί το πρόγραμμα `cvsup` το οποίο αλληλεπιδρά με ένα αντίστοιχο εξυπηρετητή `cvsupd` ώστε να ενημερώσει τα σχετικά αρχεία. Οι ενημερώσεις που λαμβάνετε είναι πάντοτε οι τελευταίες διαθέσιμες, και θα τις λάβετε μόνο όταν τις ζητήσετε. Μπορείτε εύκολα να περιορίσετε τις ενημερώσεις σε συγκεκριμένα αρχεία ή καταλόγους τα οποία σας ενδιαφέρουν. Οι ενημερώσεις δημιουργούνται δυναμικά από τον εξυπηρετητή, ανάλογα με το τι έχετε εγκατεστημένο και τι επιθυμείτε να λάβετε. Το Ανώνυμο CVS είναι κάπως πιο απλοϊκό από το CVSup, δεδομένου ότι είναι απλώς μια επέκταση του CVS που επιτρέπει την ανάκτηση αλλαγών απευθείας από κάποιο απομακρυσμένο CVS repository. Το CVSup είναι αρκετά πιο αποτελεσματικό σε αυτόν το τομέα, αλλά το Ανώνυμο CVS είναι απλούστερο στη χρήση.

Από την άλλη μεριά, το CTM δεν συγκρίνει άμεσα τον πηγαίο κώδικα που έχετε με αυτόν που υπάρχει στον κεντρικό εξυπηρετητή ώστε να ανακτήσει μόνο τις αλλαγές. Αντίθετα, στο κεντρικό μηχάνημα CTM, εκτελείται αρκετές φορές την ημέρα ένα script. Το script αυτό αναγνωρίζει τις αλλαγές στα αρχεία σε σχέση με την προηγούμενη εκτέλεση του, και έπειτα πακετάρει και συμπιέζει τις αλλαγές με τρόπο κατάλληλο για αποστολή μέσω email (μόνο εκτυπώσιμοι ASCII χαρακτήρες). Σε κάθε τέτοιο πακέτο αλλαγών αντιστοιχίζεται ένας μοναδιαίος αριθμός ακολουθίας (sequence number) που το αναγνωρίζει. Μετά τη λήψη τους, μπορείτε να δώσετε αυτά τα αρχεία διαφορών του CTM ("CTM deltas") στο βοηθητικό πρόγραμμα ctm_rmail(1) το οποίο αυτόματα θα τα αποκωδικοποιήσει, θα τα επαληθεύσει, και θα εφαρμόσει τις αλλαγές στο αντίγραφο πηγαίου κώδικα του χρήστη. Η διαδικασία αυτή είναι πολύ πιο αποδοτική από το CVSup, και επιβαρύνει λιγότερο τους εξυπηρετητές μας, καθώς είναι μια διαδικασία τύπου *push* αντί για *pull*.

Υπάρχουν φυσικά κάποια σημεία που υστερεί. Αν από λάθος διαγράψετε κάποια τμήματα του πηγαίου σας κώδικα, το CVSup θα ανιχνεύσει και θα διορθώσει αυτόματα τη βλάβη για σας. Το CTM δεν θα το κάνει αυτό, και αν σβήσετε κάποιο τμήμα του δέντρου σας (και δεν έχετε αντίγραφο ασφαλείας) θα πρέπει να ξεκινήσετε από την αρχή (από το πιο πρόσφατο CVS "base delta") και να το ξανακτίσετε από την αρχή με το CTM. Με το Ανώνυμο CVS, μπορείτε απλώς να διαγράψετε τα προβληματικά αρχεία και να συγχρονίσετε ξανά τον πηγαίο σας κώδικα.

44.7. Μεταγλωττίζοντας το Βασικό Σύστημα ("world")

Έχοντας συγχρονίσει το τοπικό σας δέντρο πηγαίου κώδικα σε κάποια συγκεκριμένη έκδοση του FreeBSD (FreeBSD-STABLE, FreeBSD-CURRENT, κ.ο.κ.), μπορείτε έπειτα να το χρησιμοποιήσετε για

να μεταγλωττίσετε το σύστημα σας από την αρχή.

Δημιουργήστε Ένα Αντίγραφο Ασφαλείας

Δεν μπορούμε παρά να τονίσουμε πόσο σημαντικό είναι να δημιουργήσετε ένα αντίγραφο ασφαλείας του συστήματος σας *πριν* ξεκινήσετε αυτή τη διαδικασία. Αν και η μεταγλώττιση του βασικού συστήματος είναι (όσο τουλάχιστον ακολουθείτε αυτές τις οδηγίες) μια σχετικά απλή διαδικασία, αναμφίβολα θα υπάρξουν και περιπτώσεις που λάθη δικά σας, ή άλλων (στο δέντρο πηγαίου κώδικα), θα σας οδηγήσουν σε ένα σύστημα που δεν θα μπορεί να εκκινήσει.

Βεβαιωθείτε ότι έχετε ενημερωμένο αντίγραφο ασφαλείας. Καλό θα είναι να έχετε επίσης πρόχειρη μια δισκέτα fixit ή ένα CD εκκίνησης. Ίσως να μην χρειαστεί ποτέ να τα χρησιμοποιήσετε, αλλά καλύτερα να είστε ασφαλής παρά να το μετανοιώνετε αργότερα!

Γίνετε Συνδρομητής στη Σωστή Λίστα Ηλ. Ταχυδρομείου

Από τη φύση τους, οι κλάδοι FreeBSD-STABLE και FreeBSD-CURRENT βρίσκονται σε συνεχή *ανάπτυξη*. Όσοι συνεισφέρουν στο FreeBSD είναι απλώς άνθρωποι, και περιστασιακά λάθη απλώς συμβαίνουν.

Ορισμένες φορές τα λάθη αυτά είναι μάλλον ακίνδυνα, και το μόνο που κάνουν είναι να εμφανίζουν μερικές διαγνωστικές προειδοποιήσεις στο σύστημα σας. Ή μπορεί η αλλαγή να είναι καταστροφική, και να οδηγήσει το σύστημα σας σε αδυναμία εκκίνησης ή ακόμα και να καταστρέψει τα συστήματα αρχείων σας (ή και ακόμα χειρότερες συνέπειες).

Αν συμβούν τέτοια προβλήματα, σύντομα θα εμφανιστεί ένα μήνυμα τύπου "heads up" στις σχετικές λίστες ταχυδρομείου, το οποίο θα εξηγεί το πρόβλημα και ποια συστήματα επηρεάζει. Όταν το πρόβλημα λυθεί, θα γίνει μια αντίστοιχη "all clear" ανακοίνωση.

Αν προσπαθείτε να ακολουθήσετε το FreeBSD-STABLE ή το FreeBSD-CURRENT, και δεν διαβάζετε τις αντίστοιχες λίστες ηλεκτρονική λίστα του FreeBSD-STABLE; και ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT, ψάχνετε για μπελάδες.

Μην Χρησιμοποιήσετε την εντολή `make world`

Μεγάλο μέρος της παλαιότερης τεκμηρίωσης, συνιστά τη χρήση της εντολής `make world`. Αν την χρησιμοποιήσετε, θα παραλειφθούν ορισμένα σημαντικά βήματα της διαδικασίας. Χρησιμοποιήστε τη μόνο αν είστε απόλυτα σίγουροι για αυτό που κάνετε. Για τις περισσότερες περιπτώσεις, η εντολή `make world` είναι λανθασμένη, και αντί για αυτή θα πρέπει να ακολουθήσετε τη διαδικασία που περιγράφουμε παρακάτω.

44.7.1. Ο Κανονικός Τρόπος να Ενημερώσετε το Σύστημα σας

Πριν ενημερώσετε το σύστημα σας, θα πρέπει να ελέγξετε το /usr/src/UPDATING για τυχόν βήματα που θα πρέπει να εκτελέσετε πριν την εκκίνηση της μεταγλώττισης. Τα βήματα αυτά εξαρτώνται

από την έκδοση του πηγαίου κώδικα που πρόκειται να χρησιμοποιήσετε. Έπειτα, ακολουθήστε τη διαδικασία που περιγράφεται στις επόμενες παραγράφους.

Η διαδικασία αναβάθμισης η οποία περιγράφεται εδώ βασίζεται στην υπόθεση ότι έχετε ήδη εγκαταστήσει μια παλιότερη έκδοση του FreeBSD, με μια παλιά έκδοση του μεταγλωττιστή, ένα παλιό πυρήνα, παλιά "εργαλεία χρήστη" και αρχεία ρυθμίσεων. Εργαλεία χρήστη θεωρούνται τα βασικά εκτελέσιμα, οι βιβλιοθήκες και τα αρχεία προγραμματισμού. Ο μεταγλωττιστής είναι κι αυτός μέρος των "εργαλείων χρήστη" στο FreeBSD, αλλά χρειάζεται ειδική μεταχείριση κατά τη διαδικασία αναβάθμισης.

Υποθέτουμε, επίσης, ότι έχετε ήδη κατεβάσει μια ενημερωμένη έκδοση από τον πηγαίο κώδικα του συστήματος. Αν ο πηγαίος κώδικας στο συγκεκριμένο σύστημα είναι από παλιότερη έκδοση, δείτε το Συγχρονίζοντας τον Πηγαίο σας Κώδικα για λεπτομερείς οδηγίες σχετικά με το πως να συγχρονίσετε τον πηγαίο κώδικα σε μια νεότερη έκδοση.

Η αναβάθμιση του FreeBSD από τον πηγαίο κώδικά του φαίνεται να είναι πολύ απλή διαδικασία. Στην πραγματικότητα, έχει κάποιες ιδιαιτερότητες. Με τα χρόνια, καθώς οι εξαρτήσεις μεταξύ των βημάτων της αναβάθμισης ανακαλύπτονται ή αναλύονται καλύτερα, οι προγραμματιστές του FreeBSD αλλάζουν σιγά-σιγά αυτή τη διαδικασία. Οι παρακάτω παράγραφοι περιγράφουν τη λογική με την οποία έχει σχεδιασθεί η προτεινόμενη διαδικασία αναβάθμισης.

Μια επιτυχής διαδικασία αναβάθμισης πρέπει να καλύψει τουλάχιστον τις δύο πιο βασικές ιδιαιτερότητες μιας αναβάθμισης από πηγαίο κώδικα:

- Ο παλιός μεταγλωττιστής συστήματος μπορεί να είναι ακατάλληλος για μεταγλώττιση του νέου πυρήνα. (Και οι μεταγλωττιστές έχουν ορισμένες φορές προβλήματα, όπως κάθε άλλο λογισμικό.) Οπότε ο νέος πυρήνας πρέπει να μεταγλωττιστεί με το νέο μεταγλωττιστή. Πιο συγκεκριμένα, ο νέος μεταγλωττιστής πρέπει να αναβαθμιστεί πριν από το νέο πυρήνα. Αυτό δε σημαίνει βέβαια ότι αυτός ο νέος μεταγλωττιστής πρέπει να *εγκατασταθεί* πριν μεταγλωττιστεί ο νέος πυρήνας.
- Τα νέα εργαλεία χρήστη από το βασικό σύστημα του FreeBSD μπορεί να εξαρτώνται από τον τρόπο λειτουργίας του νέου πυρήνα. Οπότε ο νέος πυρήνας πρέπει να εγκατασταθεί πριν από το νέο βασικό σύστημα.

Αυτά τα δύο σημεία είναι οι βασικοί λόγοι για τους οποίους προτείνονται τα κεντρικά βήματα μιας αναβάθμισης, τα βήματα `buildworld`, `buildkernel`, `installkernel`, και `installworld`. Στις επόμενες παραγράφους θα περιγράψουμε πιο αναλυτικά αυτά τα βήματα. Υπάρχουν κι άλλοι λόγοι όμως για τους οποίους χρειάζεται προσοχή όταν κάνετε μια τέτοια αναβάθμιση. Μερικοί από αυτούς είναι οι εξής:

- Τα παλιά εργαλεία του βασικού συστήματος μπορεί να μην τρέχουν σωστά με το νέο πυρήνα. Γι αυτό πρέπει να εγκατασταθεί το ενημερωμένο βασικό σύστημα αμέσως μετά την εγκατάσταση του νέου πυρήνα.
- Μερικές φορές χρειάζονται αλλαγές στα αρχεία ρυθμίσεων πριν εγκατασταθεί το νέο βασικό σύστημα. Άλλες φορές η εγκατάσταση όλων των αρχείων ρυθμίσεων μπορεί να δημιουργήσει προβλήματα στην εγκατάσταση. Γι αυτό έχουμε χωρίσει την ενημέρωση των αρχείων ρυθμίσεων σε δύο ξεχωριστά βήματα.
- Στην πλειοψηφία των περιπτώσεων η διαδικασία εγκατάστασης αντικαθιστά ή προσθέτει αρχεία

του συστήματος· δε σβήνει κανένα υπάρχον αρχείο. Σε μερικές περιπτώσεις αυτό μπορεί να δημιουργήσει προβλήματα. Όταν υπάρχει τέτοια περίπτωση, η διαδικασία εγκατάστασης τυπώνει ενημερωτικά μηνύματα για τα αρχεία τα οποία πρέπει να σβηστούν χειροκίνητα. Αυτό το βήμα μπορεί να αυτοματοποιηθεί στο μέλλον.

Έχοντας όλες αυτές τις ιδιαιτερότητες μιας αναβάθμισης από πηγαίο κώδικα, καταλήξαμε στην παρακάτω διαδικασία αναβάθμισης. Ορισμένες φορές μπορεί να χρειάζεται να προσθέσετε κάποια βήματα σε αυτή τη διαδικασία. Τα βασικά βήματα όμως παραμένουν τα ίδια, κι είναι τα εξής:

1. `make buildworld`

   Αυτό το βήμα μεταγλωττίζει πρώτα μια ενημερωμένη έκδοση του ίδιου του μεταγλωττιστή συστήματος και μερικών απαραίτητων εργαλείων. Ύστερα, χρησιμοποιώντας το νέο μεταγλωττιστή, προετοιμάζει μια νέα έκδοση όλου του βασικού συστήματος του FreeBSD. Τα ενημερωμένα εκτελέσιμα, βιβλιοθήκες και αρχεία προγραμματισμού καταλήγουν στον κατάλογο /usr/obj.

2. `make buildkernel`

   Σε αντίθεση με παλιότερες διαδικασίες αναβάθμισης (οι οποίες καλούσαν χειροκίνητα το config(8) και το make(1)) αυτό το βήμα μεταγλωττίζει τον πυρήνα του FreeBSD χρησιμοποιώντας τον ενημερωμένο μεταγλωττιστή συστήματος από τον κατάλογο /usr/obj. Αυτό σας προστατεύει από προβλήματα ασυμβατότητας μεταξύ του μεταγλωττιστή και του πυρήνα.

3. `make installkernel`

   Εγκατάσταση του νέου πυρήνα και των αρθρωμάτων του στο δίσκο του συστήματος. Έτσι μπορεί πλέον το σύστημα να ξεκινήσει με το νέο, ενημερωμένο πυρήνα.

4. Εκκίνηση σε λειτουργία single user.

   Η λειτουργία single user ελαχιστοποιεί την πιθανότητα να έχετε προβλήματα επειδή αναβαθμίσατε κάποιο πρόγραμμα που τρέχει ήδη. Είναι επίσης πιο ασφαλής, αφού δε χρειάζεται να τρέξετε τις εφαρμογές του παλιού βασικού συστήματος με το νέο πυρήνα.

5. `mergemaster -p`

   Αυτό το βήμα ενημερώνει τα απολύτως βασικά αρχεία ρυθμίσεων του FreeBSD, για να μπορέσετε να εγκαταστήσετε σωστά το νέο βασικό σύστημα. Ενημερώνει, για παράδειγμα, τη βάση χρηστών και ομάδων χρηστών του FreeBSD. Κάθε φορά που προστίθεται ένας νέος χρήστης συστήματος ή μια νέα ομάδα χρηστών, το βήμα `installworld` της αναβάθμισης θεωρεί ότι έχετε ήδη ρυθμίσει τους νέους χρήστες ή τις νέες ομάδες. Αυτό ακριβώς κάνει σε αυτό το σημείο το εργαλείο mergemaster(8).

6. `make installworld`

   Το επόμενο βήμα είναι να εγκαταστήσετε το ενημερωμένο βασικό σύστημα από τον κατάλογο /usr/obj. Μετά από αυτό έχετε πλέον ένα νέο πυρήνα και ένα ενημερωμένο βασικό σύστημα, το οποίο ταιριάζει με τον νέο πυρήνα.

7. `mergemaster`

Ένα από τα τελευταία βήματα είναι η αναβάθμιση των αρχείων ρυθμίσεων του συστήματος. Το εργαλείο mergemaster(8) μπορεί να σας βοηθήσει σε αυτό το βήμα, αφού ενημερώνει τα αρχεία ρυθμίσεων κρατώντας και οποιεσδήποτε τοπικές αλλαγές έχετε κάνει στο σύστημά σας.

8. Επανεκκινήστε το σύστημα.

   Μια τελευταία επανεκκίνηση του συστήματος σας εξασφαλίζει ότι το σύστημα ξεκινάει με το νέο πυρήνα, το ενημερωμένο βασικό σύστημα και τα καινούρια αρχεία ρυθμίσεων.

Αν η αναβάθμιση που κάνετε είναι από μια έκδοση του FreeBSD σε μια πιο καινούρια έκδοση του ίδιου κλάδου ανάπτυξης, π.χ. από 7.0 σε 7.1, τότε μερικά από τα βήματα αυτή της διαδικασίας μπορεί να μη χρειάζονται αφού είναι λιγότερο πιθανό να συναντήσετε ασυμβατότητες μεταξύ του μεταγλωττιστή συστήματος, του πυρήνα, του βασικού συστήματος και των αρχείων ρυθμίσεων. Η αναβάθμιση σε τέτοιες περιπτώσεις, μεταξύ δύο minor εκδόσεων του FreeBSD, ίσως μπορεί να γίνει και με την παλιότερη διαδικασία: τρέχοντας `make world` και ύστερα μεταγλωττίζοντας και στήνοντας ένα νέο πυρήνα.

Όταν όμως αναβαθμίσετε το FreeBSD μεταξύ major εκδόσεων, καλύτερα να χρησιμοποιήσετε τη διαδικασία που περιγράφουμε εδώ. Αλλιώς μπορεί να αντιμετωπίσετε προβλήματα είτε κατά τη διάρκεια της αναβάθμισης ή αφού έχει πλέον ολοκληρωθεί.

Κάποιες από τις αναβαθμίσεις (π.χ. από μια έκδοση 4.*X* σε 5.0) μπορεί να απαιτούν μερικά χειροκίνητα βήματα (όπως το να μετακινήσετε ή να σβήσετε συγκεκριμένα αρχεία πριν το βήμα `installworld`). Πριν από κάθε αναβάθμιση διαβάστε προσεκτικά τις οδηγίες στο αρχείο /usr/src/UPDATING· ειδικά τις οδηγίες στο τέλος του αρχείου, οι οποίες περιγράφουν αναλυτικά την προτεινόμενη διαδικασία αναβάθμισης.

Αυτή η διαδικασία αναβάθμισης εξελίσσεται και διορθώνεται καθώς οι προγραμματιστές του FreeBSD ανακαλύπτουν καινούριες εξαρτήσεις μεταξύ των συστατικών του συστήματος ή κάνουν διορθώσεις για να αποφύγουν ασυμβατότητες μεταξύ των διαφορετικών υποσυστημάτων. Ελπίζουμε ότι τα κεντρικά βήματα της διαδικασίας που περιγράφεται εδώ δε θα αλλάξουν πολύ για αρκετό καιρό πλέον.

Ανακεφαλαιώνοντας όλα τα βήματα τα οποία περιγράψαμε παραπάνω, η προτεινόμενη διαδικασία αναβάθμισης του FreeBSD από τον πηγαίο κώδικα του συστήματος είναι:

```
# cd /usr/src
# make buildworld
# make buildkernel
# make installkernel
# shutdown -r now
```

Υπάρχουν κάποιες μάλλον σπάνιες περιπτώσεις, που απαιτείται μια επιπλέον εκτέλεση του `mergemaster -p` πριν το βήμα `buildworld`. Οι περιπτώσεις αυτές περιγράφονται στο UPDATING. Σε γενικές γραμμές πάντως, μπορείτε με ασφάλεια να παραλείψετε αυτό το βήμα, αν δεν αναβαθμίζετε το σύστημα σας μεταξύ πολλαπλών εκδόσεων του FreeBSD.

Μετά την επιτυχή ολοκλήρωση του `installkernel`, θα πρέπει να επανεκκινήσετε σε κατάσταση ενός χρήστη (π.χ. χρησιμοποιώντας την εντολή `boot -s` στην προτροπή του φορτωτή εκκίνησης). Έπειτα εκτελέστε:

```
# mount -u /
# mount -a -t ufs
# adjkerntz -i
# mergemaster -p
# cd /usr/src
# make installworld
# mergemaster
# reboot
```

Διαβάστε τις Επιπλέον Εξηγήσεις

Η διαδικασία που περιγράψαμε παραπάνω είναι μια απλή περίληψη για να σας βοηθήσει να ξεκινήσετε. Θα πρέπει ωστόσο να διαβάσετε τις παρακάτω ενότητες για να κατανοήσετε πλήρως κάθε βήμα, ειδικά αν θέλετε να χρησιμοποιήσετε δικό σας προσαρμοσμένο πυρήνα.

44.7.2. Διαβάστε το /usr/src/UPDATING

Πριν κάνετε οτιδήποτε άλλο, διαβάστε το /usr/src/UPDATING (ή το αντίστοιχο αρχείο, αν έχετε αποθηκεύσει τον πηγαίο κώδικα σε άλλο κατάλογο). Το αρχείο αυτό περιέχει σημαντικές πληροφορίες σχετικά με προβλήματα που μπορεί να συναντήσετε ή ίσως να καθορίζει τη σειρά με την οποία πρέπει να εκτελεστούν κάποιες εντολές. Αν το αρχείο UPDATING έρχεται σε σύγκρουση με κάτι που διαβάσατε εδώ, προτεραιότητα έχει το αρχείο UPDATING.

Η ανάγνωση του αρχείου UPDATING δεν είναι αποδεκτό υποκατάστατο της συνδρομής στη σωστή λίστα ηλεκτρονικού ταχυδρομείου, όπως περιγράψαμε προηγουμένως. Οι δύο απαιτήσεις είναι συμπληρωματικές, δεν αλληλοαναιρούνται.

44.7.3. Ελέγξτε το /etc/make.conf

Εξετάστε τα αρχεία /usr/shared/examples/etc/make.conf και /etc/make.conf. Το πρώτο περιέχει κάποιες προεπιλεγμένες μεταβλητές (defines), οι περισσότερες από τις οποίες είναι ως σχόλια. Για να τα χρησιμοποιήσετε όταν μεταγλωττίζετε το σύστημα σας, προσθέστε τα στο /etc/make.conf. Να έχετε υπόψη σας, πως οτιδήποτε προσθέτετε στο αρχείο /etc/make.conf χρησιμοποιείτε επίσης κάθε φορά που εκτελείτε την εντολή `make`, έτσι είναι γενικά καλή ιδέα να βάλετε τιμές που είναι λογικές για το σύστημα σας.

Ένας τυπικός χρήστης θα θέλει πιθανώς να αντιγράψει τις γραμμές `CFLAGS` και `NO_PROFILE` από το αρχείο /usr/shared/examples/etc/make.conf στο /etc/make.conf αφαιρώντας ταυτόχρονα και το σύμβολο του σχολίου.

Εξετάστε και τις άλλες μεταβλητές (`COPTFLAGS`, `NOPORTDOCS` κ.ο.κ.) και αποφασίστε αν σχετίζονται με το επιθυμητό για σας αποτέλεσμα.

44.7.4. Ενημερώστε τα Αρχεία στο /etc

Ο κατάλογος /etc περιέχει μεγάλο μέρος των πληροφοριών ρύθμισης του συστήματος σας, όπως επίσης και scripts που εκτελούνται κατά την εκκίνηση του συστήματος. Μερικά από τα scripts αυτά αλλάζουν από έκδοση σε έκδοση του FreeBSD.

Ορισμένα από τα αρχεία ρυθμίσεων χρησιμοποιούνται επίσης κατά την καθημερινή χρήση του συστήματος. Το /etc/group είναι ένα από αυτά.

Έχουν υπάρξει περιπτώσεις στο παρελθόν, όπου το `make installworld` ανέμενε από πριν την ύπαρξη συγκεκριμένων ονομάτων χρηστών (usernames) ή ομάδων (groups). Κατά τη διαδικασία της αναβάθμισης ήταν αρκετά πιθανό αυτοί οι χρήστες ή ομάδες να μην υπήρχαν. Αυτό δημιουργούσε προβλήματα στην διαδικασία. Σε κάποιες περιπτώσεις, το `make buildworld` θα ελέγξει αν υπάρχουν αυτοί οι χρήστες ή ομάδες.

Μια τέτοια περίπτωση παρουσιάστηκε όταν προστέθηκε ο χρήστης `smmsp`. Η διαδικασία αναβάθμισης αποτύγχανε σε πολλούς χρήστες, τη στιγμή που το mtree(8) προσπαθούσε να δημιουργήσει τον κατάλογο /var/spool/clientmqueue.

Η λύση είναι να εκτελέσετε το mergemaster(8) σε κατάσταση προ-εγκατάστασης, δίνοντας την επιλογή `-p`. Αυτή θα συγκρίνει μόνο τα αρχεία που είναι απαραίτητα για την επιτυχία εκτέλεσης του `buildworld` ή του `installworld`.

```
# cd /usr/src/usr.sbin/mergemaster
# ./mergemaster.sh -p
```

Αν αισθάνεστε ιδιαίτερα παρανοϊκός, μπορείτε να ελέγξετε το σύστημα σας για να δείτε ποια αρχεία ανήκουν στην ομάδα που μετονομάζετε ή διαγράφετε:

```
# find / -group GID -print
```

Η παραπάνω εντολή θα σας δείξει όλα τα αρχεία τα οποία ανήκουν στην ομάδα *GID* (μπορείτε να δώσετε όνομα ή αριθμητικό αναγνωριστικό της ομάδας).

44.7.5. Μεταβείτε σε Κατάσταση Ενός Χρήστη

Ίσως προτιμάτε να μεταγλωττίσετε το σύστημα σε κατάσταση ενός χρήστη. Εκτός από το προφανές πλεονέκτημα της ελαφρά μεγαλύτερης ταχύτητας, η επανεγκατάσταση του συστήματος θα επηρεάσει πολλά σημαντικά αρχεία του συστήματος, όλα τα εκτελέσιμα αρχεία του βασικού συστήματος, τις βιβλιοθήκες, τα αρχεία include κ.α. Αν τα αλλάξετε αυτά σε ένα σύστημα που βρίσκεται σε κανονική λειτουργία (και ειδικά αν υπάρχουν ενεργοί χρήστες την δεδομένη στιγμή), ψάχνετε για μπελάδες.

Μια άλλη μέθοδος είναι να μεταγλωττίσετε το σύστημα σε κατάσταση κανονικής λειτουργίας, αλλά να μεταβείτε σε κατάσταση ενός χρήστη για την εγκατάσταση. Αν θέλετε να το κάνετε με αυτό τον τρόπο, απλώς μην εκτελέσετε τα ακόλουθα βήματα μέχρι το τέλος της μεταγλώττισης. Μπορείτε να αναβάλλετε τη μετάβαση σε κατάσταση ενός χρήστη μέχρι να είστε έτοιμοι για το `installkernel` ή

`installworld`.

Ως υπερχρήστης μπορείτε να εκτελέσετε:

```
# shutdown now
```

σε ένα σύστημα σε κανονική λειτουργία για να μεταβείτε σε κατάσταση ενός χρήστη.

Εναλλακτικά, επανεκκινήστε το σύστημα και στην προτροπή του φορτωτή εκκίνησης, επιλέξτε "single user". Το σύστημα θα ξεκινήσει σε κατάσταση ενός χρήστη. Στην προτροπή της γραμμής εντολών θα πρέπει να γράψετε:

```
# fsck -p
# mount -u /
# mount -a -t ufs
# swapon -a
```

Θα γίνει έλεγχος στα συστήματα αρχείων, και προσάρτηση του / με δυνατότητα ανάγνωσης/εγγραφής. Έπειτα θα προσαρτηθούν όλα τα άλλα συστήματα αρχείων UFS τα οποία αναφέρονται στο /etc/fstab, και θα ενεργοποιηθεί το swap.

Αν το CMOS ρολόι του υπολογιστή σας είναι ρυθμισμένο σε τοπική ώρα και όχι σε GMT (αυτό είναι αλήθεια αν η έξοδος της εντολής date(1) δεν δείχνει σωστή ημερομηνία και ώρα), ίσως χρειαστεί να εκτελέσετε επίσης την παρακάτω εντολή:

```
# adjkerntz -i
```

Με αυτό τον τρόπο θα βεβαιωθείτε ότι οι τοπικές σας ρυθμίσεις ώρας έχουν ρυθμιστεί σωστά. Διαφορετικά, μπορεί να συναντήσετε προβλήματα αργότερα.

44.7.6. Διαγράψτε το /usr/obj

Καθώς γίνεται η επαναμεταγλώττιση, τμήματα του συστήματος τοποθετούνται από προεπιλογή σε υποκαταλόγους του /usr/obj. Οι υποκατάλογοι αυτοί αντιγράφουν τη δομή που ακολουθείται στο /usr/src.

Μπορείτε να επιταχύνετε τη διαδικασία του `make buildworld` και επίσης να γλυτώσετε από κάποια πιθανά προβλήματα, αν διαγράψετε και αυτό τον κατάλογο.

Κάποια αρχεία σε υποκαταλόγους του /usr/obj μπορεί να έχουν χαρακτηριστεί ως immutable μέσω του αντίστοιχου flag (για περισσότερες λεπτομέρειες δείτε το chflags(1)). Πριν διαγράψετε αυτά τα αρχεία, θα πρέπει πρώτα να καταργήσετε αυτό το flag.

```
# cd /usr/obj
# chflags -R noschg *
```

```
# rm -rf *
```

44.7.7. Επαναμεταγλωττίστε το Βασικό Σύστημα

44.7.7.1. Αποθηκεύστε την Έξοδο

Καθώς εκτελείται η make(1), είναι καλή ιδέα η έξοδος της να αποθηκεύεται σε κάποιο άλλο αρχείο. Αν κάτι πάει στραβά, θα έχετε ένα αντίγραφο του μηνύματος λάθους. Αν και αυτό ίσως δεν σας βοηθήσει να βρείτε τι πήγε στραβά, μπορεί να διευκολύνει άλλους αν στείλετε το μήνυμα σας σε μια από τις λίστες ηλεκτρονικού ταχυδρομείου του FreeBSD.

Ο ευκολότερος τρόπος για να γίνει αυτό, είναι χρησιμοποιώντας την εντολή script(1) με μια παράμετρο που να καθορίζει το όνομα του αρχείου στο οποίο θα αποθηκευτεί η έξοδος. Θα πρέπει να το εκτελέσετε αμέσως πριν ξεκινήσετε την μεταγλώττιση του βασικού συστήματος, και να γράψετε `exit` μόλις η διαδικασία ολοκληρωθεί.

```
# script /var/tmp/mw.out
Script started, output file is /var/tmp/mw.out
# make TARGET
... μεταγλώττιση, μεταγλώττιση, μεταγλώττιση ...
# exit
Script done, ...
```

Αν αποφασίσετε να αποθηκεύσετε την έξοδο, *μη χρησιμοποιήσετε* για αυτό το σκοπό τον κατάλογο /tmp. Τα περιεχόμενα αυτού του καταλόγου πιθανώς να διαγραφούν την επόμενη φορά που θα εκκινήσετε το σύστημα σας. Ένας καλύτερος κατάλογος για την αποθήκευση του είναι ο /var/tmp (όπως στο προηγούμενο παράδειγμα) ή ο προσωπικός κατάλογος του `root`.

44.7.7.2. Μεταγλωττίστε το Βασικό Σύστημα

Θα πρέπει να βρίσκεστε στον κατάλογο /usr/src:

```
# cd /usr/src
```

(εκτός αν φυσικά έχετε αποθηκεύσει τον πηγαίο κώδικα σε κάποιο άλλο κατάλογο, οπότε απλώς μετακινηθείτε σε αυτόν).

Για να επαναμεταγλωττίσετε το βασικό σύστημα, χρησιμοποιήστε την εντολή make(1). Η εντολή αυτή διαβάζει τις σχετικές οδηγίες από το αρχείο Makefile, το οποίο περιγράφει με ποιο τρόπο πρέπει να μεταγλωττιστούν τα προγράμματα από τα οποία αποτελείται το FreeBSD, τη σειρά με την οποία πρέπει να γίνει η μεταγλώττιση κ.ο.κ.

Η γενική μορφή της εντολής που θα πληκτρολογήσετε είναι η παρακάτω:

```
# make -x -DVARIABLE target
```

Στο παράδειγμα αυτό, το `-x` αντιπροσωπεύει μια επιλογή που θέλετε να δώσετε στην make(1). Δείτε την σελίδα manual του make(1) για παραδείγματα δυνατών επιλογών.

Η επιλογή `-DVARIABLE` περνάει μια μεταβλητή στο Makefile. Η συμπεριφορά του Makefile ελέγχεται από τέτοιου είδους μεταβλητές. Πρόκειται για τις ίδιες μεταβλητές που καθορίζονται και στο /etc/make.conf, και αυτός είναι ένας ακόμα τρόπος καθορισμού τους.

```
# make -DNO_PROFILE target
```

Το παραπάνω δείχνει ένα επιπλέον τρόπο να καθορίσετε ότι δεν θέλετε να μεταγλωττιστούν οι βιβλιοθήκες με πληροφορίες profiling, και αντιστοιχεί με την παρακάτω γραμμή στο /etc/make.conf:

```
NO_PROFILE=    true     #    Avoid compiling profiled libraries
```

Το *target* δηλώνει στο make(1) τι θέλετε να κάνετε. Σε κάθε Makefile ορίζεται ένας αριθμός διαφορετικών "targets", και η επιλογή που θα κάνετε, καθορίζει τι ακριβώς θα γίνει.

Κάποια από τα targets που καθορίζονται στο Makefile, δεν προορίζονται για άμεση εκτέλεση από το χρήστη. Αντί για αυτό, χρησιμοποιούνται από τη διαδικασία μεταγλώττισης για να μοιραστεί ο αριθμός των βημάτων που απαιτούνται για τη μεταγλώττιση του συστήματος, σε ένα αριθμό υπο-βημάτων.

Στις περισσότερες περιπτώσεις δεν θα χρειαστεί να δώσετε καμία παράμετρο στο make(1), και έτσι η εντολή σας θα μοιάζει με την παρακάτω:

```
# make target
```

Όπου το *target* θα είναι μια από τις πολλές επιλογές μεταγλώττισης. Το πρώτο target θα πρέπει πάντα να είναι το `buildworld`.

Όπως εννοείται και από το όνομα, το `buildworld` μεταγλωττίζει ένα πλήρες δέντρο μέσα στον κατάλογο /usr/obj, ενώ το `installworld`, εγκαθιστά αυτό το δέντρο στο τρέχον μηχάνημα.

Η ύπαρξη διαφορετικών επιλογών, είναι χρήσιμη για δύο λόγους. Πρώτα από όλα, σας επιτρέπει να εκτελέσετε τη διαδικασία μεταγλώττισης με ασφάλεια, γνωρίζοντας ότι δεν πρόκειται να επηρεαστεί κανένα τμήμα του τρέχοντος συστήματος σας. Η διαδικασία μεταγλώττισης είναι "self hosted", απομονωμένη από την υπόλοιπη λειτουργία του μηχανήματος. Μπορείτε έτσι να εκτελέσετε το `buildworld` σε ένα μηχάνημα που βρίσκεται σε κανονική λειτουργία (πολλαπλών χρηστών) χωρίς να υπάρχει φόβος παρενεργειών. Ωστόσο, συνίσταται να εκτελέσετε το `installworld` σε κατάσταση λειτουργίας ενός χρήστη.

Ο δεύτερος λόγος είναι ότι σας επιτρέπει να χρησιμοποιήσετε προσαρτήσεις NFS για να αναβαθμίσετε πολλά μηχανήματα του δικτύου σας. Αν έχετε τρία μηχανήματα, τα `A`, `B` και `C` τα οποία θέλετε να αναβαθμίσετε, εκτελέστε το `make buildworld` και το `make installworld` στο μηχάνημα `A`. Το `B` και το `C` μπορούν να προσαρτήσουν τον κατάλογο /usr/src και τον /usr/obj από τον `A` μέσω NFS, και έπειτα μπορείτε να εκτελέσετε το `make installworld` για να εγκαταστήσετε το έτοιμο πλέον σύστημα

στον `B` και `C`.

Αν και υπάρχει ακόμα το target `world`, δεν συνίσταται πλέον η χρήση του.

Εκτελέστε την εντολή:

```
# make buildworld
```

Μπορείτε να καθορίσετε την επιλογή `-j` στην `make` ώστε να εκτελεστεί σε πολλαπλές διεργασίες. Αυτό είναι περισσότερο χρήσιμο σε μηχανήματα με πολλούς επεξεργαστές, ωστόσο καθώς το μεγαλύτερο μέρος της διαδικασίας μεταγλώττισης καθυστερεί εξαιτίας του σκληρού δίσκου (IO bound) και όχι της CPU, μπορεί να σας φανεί χρήσιμο ακόμα και σε μηχανήματα με ένα επεξεργαστή.

Σε ένα τυπικό μηχάνημα με μια CPU, θα μπορούσατε να δώσετε:

```
# make -j4 buildworld
```

Με την παραπάνω εντολή, το make(1) θα χρησιμοποιεί μέχρι 4 διεργασίες κάθε χρονική στιγμή. Από την εμπειρία που έχουμε και από ότι αναφέρουν οι χρήστες στις λίστες, φαίνεται ότι η ρύθμιση αυτή δίνει γενικά την καλύτερη απόδοση.

Αν έχετε μηχάνημα με πολλούς επεξεργαστές, και χρησιμοποιείτε πυρήνα με δυνατότητα SMP, δοκιμάστε τιμές μεταξύ του 6 και του 10 για να δείτε ποια επιταχύνει καλύτερα το αποτέλεσμα.

44.7.7.3. Χρόνος Μεταγλώττισης

Ο χρόνος που απαιτείται για την μεταγλώττιση επηρεάζεται από πολλούς παράγοντες. Ωστόσο, σε σύγχρονα μηχανήματα η διαδικασία δεν κρατάει συνήθως παραπάνω από μία ή δύο ώρες, όταν γίνεται μεταγλώττιση του δέντρου FreeBSD-STABLE, και μάλιστα χωρίς να χρειάζεται να γίνουν ειδικές ρυθμίσεις ή κόλπα. Το δέντρο FreeBSD-CURRENT χρειάζεται γενικά λίγο περισσότερο χρόνο για να μεταγλωττιστεί.

44.7.8. Μεταγλωττίστε και Εγκαταστήστε Νέο Πυρήνα

Για να εκμεταλλευθείτε πλήρως το νέο σας σύστημα, θα πρέπει να επαναμεταγλωττίσετε τον πυρήνα. Αυτό είναι πρακτικά αναγκαίο, καθώς κάποιες δομές στη μνήμη πιθανώς να έχουν αλλάξει, και έτσι προγράμματα όπως τα ps(1) και top(1) δεν θα λειτουργούν σωστά μέχρι να συγχρονίσετε τον πυρήνα με την έκδοση πηγαίου κώδικα του βασικού συστήματος.

Ο απλούστερος και πλέον ασφαλής τρόπος, είναι να μεταγλωττίσετε και να εγκαταστήσετε ένα πυρήνα βασισμένο στον GENERIC. Αν και ο GENERIC μπορεί να μην περιέχει όλες τις απαραίτητες συσκευές για το σύστημα σας, θα πρέπει να περιέχει ότι χρειάζεται ώστε να ξεκινήσετε ξανά το σύστημα σας σε κατάσταση λειτουργίας ενός χρήστη. Αυτό είναι ένα καλό τεστ σωστής λειτουργίας του συστήματος. Μετά την εκκίνηση με τον GENERIC, και αφού επαληθεύσετε τη σωστή λειτουργία του συστήματος, μπορείτε να μεταγλωττίσετε ένα νέο πυρήνα βασισμένο στο δικό σας προσαρμοσμένο αρχείο ρυθμίσεων.

Στο FreeBSD είναι σημαντικό να εκτελέσετε το build world πριν μεταγλωττίσετε νέο πυρήνα.

Αν θέλετε να μεταγλωττίσετε νέο πυρήνα, και έχετε ήδη ένα αρχείο με προσαρμοσμένες ρυθμίσεις, χρησιμοποιήστε απλώς την επιλογή `KERNCONF=MYKERNEL` με τον τρόπο που φαίνεται παρακάτω:

```
# cd /usr/src
# make buildkernel KERNCONF=MYKERNEL
# make installkernel KERNCONF=MYKERNEL
```

Σημειώστε ότι αν έχετε ανεβάσει την τιμή του `kern.securelevel` πάνω από το 1, *και* έχετε θέσει το flag `noschg` ή κάποιο αντίστοιχο στο εκτελέσιμο αρχείο του πυρήνα, μάλλον θα χρειαστεί να μεταβείτε σε κατάσταση λειτουργίας ενός χρήστη για να χρησιμοποιήσετε το `installkernel`. Διαφορετικά, μπορείτε να εκτελέσετε και τις δύο αυτές εντολές από την κανονική κατάσταση λειτουργίας (πολλών χρηστών) χωρίς να δημιουργηθούν προβλήματα. Δείτε τη σελίδα manual του init(8) για λεπτομέρειες σχετικά με τη ρύθμιση `kern.securelevel` και τη σελίδα του chflags(1) για λεπτομέρειες σχετικά με τα διάφορα flags που χρησιμοποιούνται σε αρχεία.

44.7.9. Επανεκκινήστε σε Κατάσταση Λειτουργίας Ενός Χρήστη

Θα πρέπει να επανεκκινήσετε σε κατάσταση λειτουργίας ενός χρήστη για να επαληθεύσετε τη λειτουργία του νέου πυρήνα. Για το σκοπό αυτό, χρησιμοποιήστε τις οδηγίες που είδαμε στο Μεταβείτε σε Κατάσταση Ενός Χρήστη.

44.7.10. Εγκαταστήστε τα Νέα Εκτελέσιμα του Συστήματος

Θα πρέπει τώρα να χρησιμοποιήσετε το `installworld` για να εγκαταστήσετε τα νέα εκτελέσιμα του συστήματος.

Εκτελέστε τις παρακάτω εντολές:

```
# cd /usr/src
# make installworld
```

Αν έχετε καθορίσει μεταβλητές στη γραμμή εντολών του `make buildworld` θα πρέπει να καθορίσετε τις ίδιες μεταβλητές και στην γραμμή εντολών του `make installworld`. Αυτό δεν είναι απαραίτητα αλήθεια για άλλες επιλογές. Για παράδειγμα, η επιλογή `-j` δεν πρέπει ποτέ να χρησιμοποιείτε με το `installworld`.

Για παράδειγμα αν εκτελέσετε:

```
# make -DNO_PROFILE buildworld
```

Θα πρέπει να εγκαταστήσετε το αποτέλεσμα χρησιμοποιώντας:

```
# make -DNO_PROFILE installworld
```

διαφορετικά το make(1) θα προσπαθήσει να εγκαταστήσει βιβλιοθήκες με profiling, τις οποίες όμως δεν μεταγλωττίσατε κατά τη διάρκεια της φάσης `make buildworld`.

44.7.11. Ενημερώστε Όσα Αρχεία δεν Ενημερώθηκαν από το `make installworld`

Η επαναμεταγλώττιση του βασικού συστήματος δεν θα ενημερώσει ορισμένους καταλόγους (ειδικότερα τους /etc, /var και /usr) με τα νέα ή αλλαγμένα αρχεία ρυθμίσεων.

Ο απλούστερος τρόπος για να ενημερώσετε τα αρχεία αυτά είναι να χρησιμοποιήσετε το mergemaster(8), αν και μπορείτε να το κάνετε και χειροκίνητα αν προτιμάτε. Άσχετα από τον τρόπο που θα προτιμήσετε, βεβαιωθείτε ότι έχετε πάρει αντίγραφο ασφαλείας του /etc σε περίπτωση που κάτι πάει στραβά.

44.7.11.1. `mergemaster`

Το βοηθητικό πρόγραμμα mergemaster(8) είναι ένα Bourne script το οποίο θα σας βοηθήσει να καθορίσετε τις διαφορές μεταξύ των εγκατεστημένων στο /etc αρχείων ρυθμίσεων, και των αντίστοιχων στο δέντρο πηγαίου κώδικα στο /usr/src/etc. Αυτή είναι και η συνιστώμενη λύση για να ενημερώσετε τα αρχεία ρυθμίσεων του συστήματος με τυχόν αλλαγές που έχουν γίνει στον νέο πηγαίο κώδικα.

Για να ξεκινήσετε, απλώς γράψτε `mergemaster` στην προτροπή της γραμμής εντολών και παρακολουθήστε την καθώς λειτουργεί. Το `mergemaster` θα δημιουργήσει ένα προσωρινό περιβάλλον root, από το / και κάτω, και θα το γεμίσει με διάφορα αρχεία ρυθμίσεων του συστήματος. Έπειτα θα γίνει σύγκριση αυτών των αρχείων με τα αντίστοιχα που βρίσκονται ήδη εγκατεστημένα στο σύστημα σας. Στο σημείο αυτό, θα σας δείξει τα αρχεία που διαφέρουν με μορφή diff(1), όπου οι γραμμές που έχουν τροποποιηθεί ή είναι νέες θα φαίνονται με ένα `+`, ενώ με το `-` θα φαίνονται οι γραμμές που είτε αφαιρούνται εντελώς ή που αντικαθίστανται από μια νέα γραμμή. Δείτε τη σελίδα manual του diff(1) για περισσότερες πληροφορίες σχετικά με τη σύνταξη του diff(1) και για τον τρόπο με τον οποίο φαίνονται οι διαφορές μεταξύ των αρχείων.

Το mergemaster(8) θα σας δείξει έπειτα κάθε αρχείο που παρουσιάζει διαφορές, και στο σημείο αυτό θα έχετε την δυνατότητα είτε να διαγράψετε το νέο αρχείο (το οποίο αναφέρεται ως προσωρινό αρχείο), είτε να εγκαταστήσετε το προσωρινό αρχείο χωρίς να κάνετε σε αυτό καμιά αλλαγή, είτε να συγχωνεύσετε τις αλλαγές των δύο αρχείων, ή τέλος να ξαναδείτε τις διαφορές μέσω της diff(1).

Αν επιλέξετε να διαγράψετε το προσωρινό αρχείο, το mergemaster(8) θα καταλάβει ότι επιθυμείτε να διατηρήσετε το τρέχον αρχείο σας χωρίς αλλαγές, και να διαγράψετε τη νέα έκδοση. Η επιλογή αυτή γενικά δεν συνίσταται, εκτός αν δεν βλέπετε κανένα λόγο να αλλάξετε το τρέχον αρχείο. Μπορείτε να δείτε βοήθεια οποιαδήποτε στιγμή κατά τη διάρκεια της διαδικασίας, πληκτρολογώντας `?` στην προτροπή του mergemaster(8). Αν αποφασίσετε να παραλείψετε κάποιο αρχείο, αυτό θα εμφανιστεί ξανά μετά το τέλος όλων των άλλων αρχείων.

Αν επιλέξετε να εγκαταστήσετε το προσωρινό αρχείο χωρίς αλλαγές, αυτό θα αντικαταστήσει το ήδη

εγκατεστημένο σας αρχείο. Αυτή είναι και η καλύτερη επιλογή για τα αρχεία τα οποία δεν έχετε αλλάξει εσείς χειροκίνητα.

Αν επιλέξετε να συγχωνεύσετε τα δύο αρχεία, θα εμφανιστεί ένας επεξεργαστής κειμένου με τα περιεχόμενα και των δύο αρχείων. Μπορείτε τώρα να τα συγχωνεύσετε παρατηρώντας ταυτόχρονα και τα δύο αρχεία δίπλα-δίπλα, και επιλέγοντας τμήματα και από τα δύο για να δημιουργήσετε την τελική έκδοση. Κατά τη σύγκριση αυτή, μπορείτε να χρησιμοποιήσετε το πλήκτρο `l` για να επιλέξετε τα περιεχόμενα που φαίνονται στην αριστερή πλευρά, ή το `r` για τα αντίστοιχα περιεχόμενα στη δεξιά. Το τελικό αποτέλεσμα θα είναι ένα αρχείο που θα αποτελείται από τμήματα και των δύο αρχείων, και το οποίο μπορείτε να εγκαταστήσετε. Η επιλογή αυτή χρησιμοποιείται συνήθως για αρχεία των οποίων το περιεχόμενο έχει μεταβληθεί από το χρήστη.

Αν επιλέξετε να δείτε ξανά τις διαφορές μέσω της diff(1), αυτές θα εμφανιστούν ακριβώς όπως έγινε και πριν σας ρωτήσει το mergemaster(8) να επιλέξετε τι θέλετε να κάνετε με το αρχείο.

Μόλις ολοκληρωθεί η λειτουργία του mergemaster(8) στα αρχεία συστήματος, θα σας ρωτήσει για άλλες επιλογές. Το mergemaster(8) ίσως σας ρωτήσει αν θέλετε να αναδημιουργήσετε το αρχείο των κωδικών (password file), και θα τελειώσει δίνοντας σας την επιλογή να διαγράψετε τυχόν προσωρινά αρχεία που δημιουργήθηκαν κατά την διαδικασία.

44.7.11.2. Χειροκίνητη Ενημέρωση

Αν επιθυμείτε να κάνετε την ενημέρωση χειροκίνητα, δεν μπορείτε απλώς να αντιγράψετε τα αρχεία από τον κατάλογο /usr/src/etc στον /etc και να περιμένετε ότι το σύστημα σας θα λειτουργήσει σωστά. Κάποια από αυτά τα αρχεία θα πρέπει να "εγκατασταθούν" πρώτα. Αυτό συμβαίνει επειδή ο κατάλογος /usr/src/etc*δεν είναι* κανονικό αντίγραφο του /etc. Επιπρόσθετα, υπάρχουν αρχεία τα οποία πρέπει να βρίσκονται στον κατάλογο /etc, αλλά δεν υπάρχουν στον /usr/src/etc.

Αν χρησιμοποιείτε το mergemaster(8) (όπως και συνίσταται), μπορείτε να διαβάσετε κατευθείαν την επόμενη ενότητα.

Ο απλούστερος τρόπος να το κάνετε αυτό χειροκίνητα, είναι να εγκαταστήσετε τα αρχεία σε ένα νέο κατάλογο, και έπειτα να τα εξετάσετε ένα-ένα ψάχνοντας για τις αλλαγές.

Κρατήστε Ένα Αντίγραφο Ασφαλείας του Καταλόγου /etc

Αν και θεωρητικά, τίποτα δεν πρόκειται να πειράξει αυτό τον κατάλογο αυτόματα, είναι πάντα καλύτερα να είμαστε σίγουροι. Για το λόγο αυτό, αντιγράψτε τον υπάρχοντα κατάλογο /etc σε κάποιο ασφαλές μέρος. Χρησιμοποιήστε μια εντολή όπως η παρακάτω:

```
# cp -Rp /etc /etc.old
```

Η επιλογή `-R` πραγματοποιεί αναδρομική αντιγραφή, ενώ η `-p` διατηρεί τα δικαιώματα, την ιδιοκτησία, τις ημερομηνίες των αρχείων, κ.ο.κ.

θα πρέπει να δημιουργήσετε μια ψευτο-δομή καταλόγων για να εγκαταστήσετε το νέο κατάλογο /etc και άλλα αρχεία. Μια λογική επιλογή είναι ο κατάλογος /var/tmp/root, και κάτω από αυτόν, θα πρέπει επίσης να δημιουργήσετε και μια ολόκληρη σειρά από τους υποκαταλόγους που απαιτούνται.

```
# mkdir /var/tmp/root
# cd /usr/src/etc
# make DESTDIR=/var/tmp/root distrib-dirs distribution
```

Οι παραπάνω εντολές θα δημιουργήσουν την απαιτούμενη δομή καταλόγων και θα εγκαταστήσουν τα αρχεία. Μεγάλο μέρος των υποκαταλόγων που έχουν δημιουργηθεί κάτω από τον /var/tmp/root είναι άδειοι, και πρέπει να διαγραφούν. Ο απλούστερος τρόπος για να γίνει αυτό, φαίνεται παρακάτω:

```
# cd /var/tmp/root
# find -d . -type d | xargs rmdir 2/dev/null
```

Αυτό θα διαγράψει όλους τους άδειους υποκαταλόγους. (Η έξοδος σφάλματος ανακατευθύνεται στο /dev/null ώστε να μην εμφανίζονται στην οθόνη προειδοποιήσεις για καταλόγους που δεν είναι άδειοι.)

Τώρα, ο /var/tmp/root περιέχει όλα τα αρχεία που θα πρέπει να τοποθετηθούν σε κατάλληλες θέσεις κάτω από τον /. Θα πρέπει τώρα να διατρέξετε καθένα από αυτά τα αρχεία, και να καθορίσετε πως καθένα από αυτά διαφέρει από το αντίστοιχο υπάρχον (εγκατεστημένο) αρχείο.

Σημειώστε ότι κάποια από τα αρχεία τα οποία έχουν εγκατασταθεί στον /var/tmp/root έχουν μια αρχική ".". Τη στιγμή που γράφονται αυτές οι γραμμές, τα μόνα αρχεία στα οποία συμβαίνει αυτό είναι τα αρχεία εκκίνησης του κελύφους στον κατάλογο /var/tmp/root/ και /var/tmp/root/root/, αν και μπορεί να υπάρχουν και άλλα (ανάλογα με το πότε διαβάζετε το κείμενο). Βεβαιωθείτε ότι χρησιμοποιείτε την εντολή `ls -a` για να τα δείτε όλα.

Ο απλούστερος τρόπος για να συγκρίνετε δύο αρχεία, είναι να χρησιμοποιήσετε την εντολή diff(1):

```
# diff /etc/shells /var/tmp/root/etc/shells
```

Η παραπάνω εντολή θα σας δείξει τις διαφορές μεταξύ του αρχείου /etc/shells και του νέου αρχείου /var/tmp/root/etc/shells. Χρησιμοποιήστε τις διαφορές αυτές για να αποφασίσετε αν θα πρέπει να συγχωνεύσετε τις αλλαγές που έχετε κάνει, ή απλώς να αντιγράψετε το παλιό σας αρχείο πάνω από το νέο.

Προσθέστε την Ημερομηνία στο Όνομα του Νέου Root Καταλόγου, (/var/tmp/root) Ώστε να Μπορείτε Εύκολα να Συγκρίνετε Διαφορετικές Εκδόσεις Μεταξύ τους

Αν μεταγλωττίζετε συχνά το βασικό σύστημα, θα πρέπει επίσης να ενημερώνετε συχνά τον κατάλογο /etc, το οποίο μπορεί να είναι ενοχλητικό.

Μπορείτε να επιταχύνετε αυτή τη διαδικασία, τηρώντας ένα αντίγραφο του τελευταίου σετ αλλαγμένων αρχείων τα οποία συγχωνεύσατε στον κατάλογο /etc. Η παρακάτω διαδικασία θα σας δώσει μια ιδέα για το πως μπορεί να γίνει αυτό:

1. Μεταγλωττίστε το βασικό σύστημα όπως κάνετε συνήθως. Όταν θέλετε να ενημερώσετε τον /etc και τους άλλους καταλόγους, δώστε στον κατάλογο

προορισμού ένα όνομα βασισμένο στην τρέχουσα ημερομηνία. Αν το κάνατε αυτό στις 14 Φεβρουαρίου 1998, θα γράφατε κάτι σαν το παρακάτω:

```
# mkdir /var/tmp/root-19980214
# cd /usr/src/etc
# make DESTDIR=/var/tmp/root-19980214 \
    distrib-dirs distribution
```

2. Συγχωνεύστε τις αλλαγές από αυτό τον κατάλογο, με τον τρόπο που περιγράψαμε παραπάνω.

   Μην διαγράψετε τον κατάλογο /var/tmp/root-19980214 όταν τελειώσετε με την παραπάνω διαδικασία.

3. Όταν κατεβάσετε την τελευταία έκδοση του πηγαίου κώδικα και τον μεταγλωττίσετε ξανά, ακολουθήστε το βήμα 1. Αυτό θα σας δώσει ένα κατάλογο που μπορεί να ονομάζεται /var/tmp/root-19980221 (αν ανάμεσα στις δύο μεταγλωττίσεις παρεμβάλλεται διάστημα μιας εβδομάδας).
4. Μπορείτε τώρα να δείτε τις διαφορές που υπάρχουν ανάμεσα στις δύο εβδομάδες, χρησιμοποιώντας την εντολή diff(1) σε αναδρομική λειτουργία για να δημιουργήσετε τις διαφορές μεταξύ των δύο καταλόγων:

   ```
   # cd /var/tmp
   # diff -r root-19980214 root-19980221
   ```

   Τυπικά, αυτό το σετ αλλαγών θα είναι πολύ μικρότερο από αυτό μεταξύ του /var/tmp/root-19980221/etc και του /etc. Καθώς αυτό το σετ αλλαγών είναι μικρότερο, είναι και πιο εύκολο να εφαρμόσετε αυτές τις αλλαγές στον κατάλογο /etc.

5. Μπορείτε τώρα να διαγράψετε τον παλιότερο από τους δύο καταλόγους /var/tmp/root-*:

   ```
   # rm -rf /var/tmp/root-19980214
   ```

6. Επαναλάβετε αυτή τη διαδικασία κάθε φορά που θέλετε να συγχωνεύσετε τις αλλαγές στον κατάλογο /etc.

Μπορείτε επίσης να χρησιμοποιήσετε την εντολή date(1) για να αυτοματοποιήσετε την δημιουργία των ονομάτων καταλόγων:

```
# mkdir /var/tmp/root-`date "+%Y%m%d"`
```

44.7.12. Επανεκκίνηση

Η διαδικασία έχει πλέον ολοκληρωθεί. Αφού επαληθεύσετε ότι όλα βρίσκονται στις σωστές θέσεις, μπορείτε να επανεκκινήσετε το σύστημα. Μια απλή εντολή shutdown(8) είναι επαρκής:

```
# shutdown -r now
```

44.7.13. Ολοκλήρωση

Έχετε πλέον αναβαθμίσει το FreeBSD σύστημα σας. Συγχαρητήρια.

Αν τα πράγματα δεν πήγαν εντελώς σωστά, είναι εύκολο να μεταγλωττίσετε ξανά οποιοδήποτε τμήμα του συστήματος. Για παράδειγμα, αν διαγράψετε κατά λάθος το /etc/magic ως μέρος μιας αναβάθμισης ή συγχώνευσης του /etc, η εντολή file(1) θα σταματήσει να λειτουργεί. Στην περίπτωση αυτή, η διόρθωση είναι να εκτελέσετε:

```
# cd /usr/src/usr.bin/file
# make all install
```

44.7.14. Ερωτήσεις

44.7.14.1. Πρέπει να μεταγλωττίσω ξανά ολόκληρο το βασικό σύστημα σε κάθε αλλαγή;

Δεν υπάρχει εύκολη απάντηση σε αυτό το ερώτημα, καθώς εξαρτάται από τη φύση της αλλαγής. Για παράδειγμα, αν εκτελέσετε το CVSup, και δείτε ότι ενημερώθηκαν τα παρακάτω αρχεία:

```
src/games/cribbage/instr.c
src/games/sail/pl_main.c
src/release/sysinstall/config.c
src/release/sysinstall/media.c
src/shared/mk/bsd.port.mk
```

Το πιθανότερο είναι ότι δεν χρειάζεται να μεταγλωττίσετε ξανά όλο το βασικό σύστημα. Μπορείτε απλώς να μεταβείτε στους σχετικούς υποκαταλόγους και να εκτελέσετε το `make all install`, και θα έχετε τελειώσει. Αν όμως υπάρχει κάποια σημαντική αλλαγή, για παράδειγμα το src/lib/libc/stdlib, θα πρέπει είτε να επαναμεταγλωττίσετε το βασικό σύστημα, ή τουλάχιστον αυτά τα κομμάτια τα οποία είναι στατικά συνδεδεμένα (όπως και οτιδήποτε άλλο έχετε προσθέσει εσείς και το οποίο είναι στατικά συνδεδεμένο).

Τελικά, η απόφαση είναι δική σας. Μπορεί να είστε ικανοποιημένος αν μεταγλωττίζετε το βασικό σύστημα κάθε δύο βδομάδες, αφήνοντας τις αλλαγές να συγκεντρωθούν στη διάρκεια αυτού του διαστήματος. Ή μπορεί να θέλετε να μεταγλωττίσετε μόνο τις αλλαγές, αν έχετε την πεποίθηση ότι μπορείτε να εντοπίσετε όλες τις εξαρτήσεις τους.

Και φυσικά, όλα αυτά εξαρτώνται από το πόσο συχνά θέλετε να ενημερώνετε το σύστημα σας, και από το αν ακολουθείτε το FreeBSD-STABLE ή το FreeBSD-CURRENT.

44.7.14.2. Η μεταγλώττιση μου απέτυχε με πλήθος μηνυμάτων signal 11signal 11 (ή λάθη με άλλα σήματα). Τι έχει συμβεί;

Αυτό συνήθως δείχνει προβλήματα υλικού. Η διαδικασία μεταγλώττισης του βασικού συστήματος είναι ένας αποτελεσματικός τρόπος να δοκιμάσετε το υλικό σας στα όρια του, και συχνά θα δείξει προβλήματα που σχετίζονται με τη μνήμη. Το πιο σύνηθες σύμπτωμα, είναι η απότομη διακοπή της μεταγλώττισης, με τον μεταγλωττιστή να φαίνεται ότι έχει λάβει κάποιο μυστηριώδες σήμα.

Ένα σίγουρο σημάδι για το παραπάνω, είναι να επανεκκινήσετε τη διαδικασία, και αυτή να σταματήσει σε διαφορετικό σημείο.

Στην περίπτωση αυτή, δεν υπάρχουν και πολλά που μπορείτε να κάνετε, εκτός από το να αρχίσετε να αλλάζετε εξαρτήματα στο μηχάνημα σας μέχρι να βρείτε αυτό που είναι υπαίτιο.

44.7.14.3. Μπορώ να διαγράψω το /usr/obj όταν τελειώσω;

Η σύντομη απάντηση είναι ναι.

Το /usr/obj περιέχει όλα τα αντικειμενικά αρχεία που παράγονται κατά τη διάρκεια της μεταγλώττισης. Συνήθως, ένα από τα πρώτα βήματα στην διαδικασία `make buildworld` είναι η διαγραφή αυτού του καταλόγου και η αναδημιουργία του. Στην περίπτωση αυτή, το να κρατήσετε τον κατάλογο /usr/obj αφού έχετε τελειώσει, δεν έχει και πολύ νόημα, ενώ αν τον σβήσετε θα κερδίσετε ένα μεγάλο κομμάτι ελεύθερου χώρου (την παρούσα στιγμή περίπου 2 GB).

Όμως, αν ξέρετε τι κάνετε, μπορείτε να οδηγήσετε το `make buildworld` να παραλείψει αυτό το βήμα. Αυτό θα επιταχύνει ιδιαίτερα τις νέες μεταγλωττίσεις, καθώς τα περισσότερα τμήματα του πηγαίου κώδικα δεν θα χρειάζονται ξανά μεταγλώττιση. Το μειονέκτημα είναι ότι ορισμένες φορές εμφανίζονται προβλήματα που έχουν σχέση με όχι και τόσο εμφανείς εξαρτήσεις, και μπορεί να οδηγήσουν σε μυστηριώδη αποτυχία της μεταγλώττισης. Τέτοια προβλήματα συχνά δημιουργούν "θόρυβο" στις λίστες του FreeBSD, όταν κάποιος χρήστης παραπονιέται ότι η μεταγλώττιση του αποτυγχάνει, χωρίς να αντιλαμβάνεται ότι αυτό οφείλεται στην προσπάθεια του να συντομεύσει την διαδικασία.

44.7.14.4. Μπορώ να συνεχίσω μια μεταγλώττιση που διέκοψα;

Αυτό εξαρτάται από το πόσο έχετε προχωρήσει στη διαδικασία μέχρι τη στιγμή που βρήκατε το πρόβλημα.

Σε γενικές γραμμές (και αυτός δεν είναι κανόνας που ισχύει πάντα), η διεργασία του `make buildworld` μεταγλωττίζει νέα αντίγραφα βασικών εργαλείων (όπως τα gcc(1), και make(1)) καθώς και των βιβλιοθηκών συστήματος. Έπειτα εγκαθιστώνται αυτά τα εργαλεία και οι βιβλιοθήκες. Τα νέα εργαλεία και βιβλιοθήκες χρησιμοποιούνται έπειτα για να επαναμεταγλωττίσουν τους εαυτούς τους, και εγκαθίστανται ξανά. Ολόκληρο το σύστημα (το οποίο τώρα περιλαμβάνει και τα συνηθισμένα προγράμματα χρήστη όπως το ls(1) ή το grep(1)) επαναμεταγλωττίζεται χρησιμοποιώντας τα νέα αρχεία του συστήματος.

Αν βρίσκεστε στο τελευταίο στάδιο, το οποίο θα το γνωρίζετε κοιτάζοντας την έξοδο που έχετε αποθηκεύσει, είναι σχετικά ασφαλές να κάνετε:

```
... fix the problem ...
```

```
# cd /usr/src
# make -DNO_CLEAN all
```

Με τον τρόπο αυτό δεν θα αναιρέσετε την εργασία που έχει γίνει από το προηγούμενο `make buildworld`.

Αν δείτε το μήνυμα:

```
----------------------------------------------------------
Building everything..
----------------------------------------------------------
```

στην έξοδο της εντολής `make buildworld`, τότε είναι μάλλον ασφαλές να προχωρήσετε με αυτό τον τρόπο.

Αν δεν δείτε αυτό το μήνυμα, ή αν δεν είστε σίγουρος, τότε είναι καλύτερα να κάνετε πλήρη μεταγλώττιση παρά να μετανιώνετε αργότερα.

44.7.14.5. Πως μπορώ να επιταχύνω τη μεταγλώττιση του βασικού συστήματος;

- Εκτελέστε την σε κατάσταση ενός χρήστη.
- Βάλτε τους καταλόγους /usr/src και /usr/obj σε διαφορετικά συστήματα αρχείων τα οποία βρίσκονται και σε διαφορετικούς φυσικούς δίσκους. Αν είναι δυνατόν, βάλτε αυτούς τους δίσκους σε χωριστούς ελεγκτές.
- Ακόμα καλύτερα, μοιράστε αυτά τα συστήματα αρχείων σε πολλαπλούς δίσκους, χρησιμοποιώντας το πρόγραμμα οδήγησης ccd(4) (concatenated disk driver, οδήγησης συνενωμένων δίσκων).
- Απενεργοποιήστε το profiling (θέστε την μεταβλητή "NO_PROFILE=true" στο /etc/make.conf). Είναι σχεδόν σίγουρο ότι δεν το χρειάζεστε.
- Στο αρχείο /etc/make.conf, θέστε το `CFLAGS` σε κάτι όπως `-O -pipe`. Η βελτιστοποίηση `-O2` χρειάζεται αρκετά περισσότερο χρόνο, και η διαφορά απόδοσης μεταξύ `-O` και `-O2` είναι συνήθως αμελητέα. Το `-pipe` επιτρέπει στον μεταγλωττιστή να χρησιμοποιήσει pipes για επικοινωνία αντί για προσωρινά αρχεία. Αυτό καταναλώνει περισσότερη μνήμη, αλλά χρησιμοποιεί λιγότερο το σκληρό δίσκο.
- Χρησιμοποιήστε την επιλογή `-jn` στο make(1) ώστε να εκτελούνται παράλληλα πολλαπλές διεργασίες μεταγλώττισης. Αυτό συνήθως βοηθάει ακόμα και σε περίπτωση που έχετε μηχάνημα με ένα επεξεργαστή.
- Μπορείτε να προσαρτήσετε (ή να επαναπροσαρτήσετε) το σύστημα αρχείων στο οποίο είναι αποθηκευμένο το /usr/src με την επιλογή `noatime`. Αυτό αποτρέπει την καταγραφή ημερομηνίας / ώρας πρόσβασης στο σύστημα αρχείων. Κατά πάσα πιθανότητα, δεν χρειάζεστε αυτή την πληροφορία έτσι και αλλιώς.

  ```
  # mount -u -o noatime /usr/src
  ```

Το παράδειγμα προϋποθέτει ότι έχετε το /usr/src στο δικό του σύστημα αρχείων. Αν αυτό δεν συμβαίνει (αν είναι μέρος του /usr για παράδειγμα) θα χρειαστεί να χρησιμοποιήσετε αυτό το σημείο προσάρτησης, και όχι το /usr/src.

- Μπορείτε να προσαρτήσετε (ή να επαναπροσαρτήσετε) το σύστημα αρχείων που περιέχει το /usr/obj με την επιλογή `async`. Με τον τρόπο αυτό, οι εγγραφές στο δίσκο θα γίνονται ασύγχρονα. Με άλλα λόγια, οι εγγραφές φαίνεται ότι ολοκληρώνονται άμεσα, ενώ η πραγματική εγγραφή στο δίσκο γίνεται λίγα δευτερόλεπτα αργότερα. Αυτό επιτρέπει την ομαδοποίηση των εγγραφών, το οποίο μπορεί να προσφέρει δραματική βελτίωση απόδοσης.

Να έχετε υπόψιν σας ότι αυτή η επιλογή μπορεί να κάνει το σύστημα αρχείων σας πολύ πιο ευαίσθητο. Με την επιλογή αυτή, υπάρχει αυξημένη πιθανότητα το σύστημα αρχείων να βρεθεί σε μη επισκευάσιμη κατάσταση αν υπάρξει διακοπή ρεύματος.

Αν το σύστημα αρχείων περιέχει μόνο το /usr/obj, το παραπάνω δεν είναι πρόβλημα. Αν ωστόσο έχετε και άλλα πολύτιμα δεδομένα στο ίδιο σύστημα αρχείων, σιγουρευτείτε ότι έχετε ενημερωμένα αντίγραφα ασφαλείας πριν ενεργοποιήσετε αυτή την επιλογή.

```
# mount -u -o async /usr/obj
```

Όπως και προηγουμένως, αν το /usr/obj δεν είναι σύστημα αρχείων από μόνο του, αντικαταστήστε το στο παράδειγμα με το όνομα του πραγματικού σημείου προσάρτησης.

44.7.14.6. Τι να κάνω αν κάτι πάει στραβά;

Σιγουρευτείτε ότι το περιβάλλον σας δεν έχει υπολείμματα από προηγούμενες μεταγλωττίσεις. Αυτό είναι αρκετά απλό.

```
# chflags -R noschg /usr/obj/usr
# rm -rf /usr/obj/usr
# cd /usr/src
# make cleandir
# make cleandir
```

Ναι, θα πρέπει να εκτελέσετε το `make cleandir` δύο φορές.

Επανεκκινήστε έπειτα όλη τη διαδικασία, ξεκινώντας με το `make buildworld`.

Αν έχετε ακόμα προβλήματα, στείλτε το μήνυμα λάθους και την έξοδο του `uname -a` στην ηλεκτρονική λίστα γενικών ερωτήσεων του FreeBSD. Να είστε προετοιμασμένοι να απαντήσετε επιπλέον ερωτήσεις σχετικά με την εγκατάσταση σας!

44.8. Διαγραφή Παρωχημένων Αρχείων, Καταλόγων και Βιβλιοθηκών

Κατά την συνεχή ανάπτυξη του FreeBSD είναι φυσιολογικό κάποια αρχεία κατά καιρούς να χαρακτηρίζονται ως παρωχημένα. Αυτό μπορεί να συμβεί αν οι λειτουργίες που παρείχαν υλοποιούνται πλέον διαφορετικά, αν ο ο αριθμός έκδοσης της βιβλιοθήκης έχει αλλάξει ή ακόμα και αν έχει διαγραφεί οριστικά από το σύστημα. Στα αρχεία αυτά περιλαμβάνονται επίσης βιβλιοθήκες κατάλογοι που πρέπει να διαγραφούν όταν γίνεται αναβάθμιση του συστήματος. Το όφελος για το χρήστη είναι ότι το σύστημα του δεν γεμίζει από παλιά αρχεία τα οποία καταλαμβάνουν άχρηστο χώρο στο μέσο αποθήκευσης και στο backup. Επιπρόσθετα, αν κάποια παλιά βιβλιοθήκη είχε προβλήματα σταθερότητας ή ασφάλειας θα πρέπει να την αναβαθμίσετε για να κρατήσετε το σύστημα σας σταθερό και ασφαλές. Τα αρχεία, οι κατάλογοι και οι βιβλιοθήκες που θεωρούνται παρωχημένες φαίνονται στο /usr/src/ObsoleteFiles.inc. Οι παρακάτω οδηγίες θα σας βοηθήσουν να διαγράψετε αυτά τα αρχεία κατά τη διαδικασία αναβάθμισης του συστήματος.

Υποθέτουμε ότι χρησιμοποιείτε τα βήματα που περιγράφονται στο Ο Κανονικός Τρόπος να Ενημερώσετε το Σύστημα σας. Μετά την επιτυχή εκτέλση της εντολής `make installworld` και του `mergemaster` που ακολουθεί, θα πρέπει να ελέγξετε για παρωχημένα αρχεία και βιβλιοθήκες όπως φαίνεται παρακάτω:

```
# cd /usr/src
# make check-old
```

Αν βρεθούν παρωχημένα αρχεία, μπορείτε να τα διαγράψετε με τις παρακάτω εντολές:

```
# make delete-old
```

Δείτε το /usr/src/Makefile για περισσότερες ενδιαφέρουσες επιλογές της `make`.

Για κάθε αρχείο που θα διαγραφεί, θα σας ζητηθεί να επιβεβαιώσετε την ενέργεια. Μπορείτε να παραλείψετε την ερώτηση και να αφήσετε το σύστημα να διαγράψει αυτά τα αρχεία αυτόματα χρησιμοποιώντας την μεταβλητή του make `BATCH_DELETE_OLD_FILES` με τον τρόπο που φαίνεται παρακάτω:

```
# make -DBATCH_DELETE_OLD_FILES delete-old
```

Η διαγραφή παρωχημένων αρχείων, θα προκαλέσει δυσλειτουργία των εφαρμογών που εξακολουθούν να βασίζονται σε αυτά. Αυτό συμβαίνει ιδιαίτερα σε παλιές βιβλιοθήκες. Στις περισσότερες περιπτώσεις, θα πρέπει να επαναμεταγλωττίσετε τα προγράμματα, ports ή βιβλιοθήκες που χρησιμοποιούσαν την παλιά βιβλιοθήκη πριν εκτελέσετε την εντολή `make delete-old-libs`.

Μπορείτε να βρείτε προγράμματα που ελέγχουν τις εξαρτήσεις των κοινόχρηστων βιβλιοθηκών στη Συλλογή των Ports, στο sysutils/libchk ή sysuilts/bsdadminscripts.

Οι παρωχημένες κοινόχρηστες βιβλιοθήκες μπορούν να δημιουργήσουν προβλήματα λόγω συγκρούσεων με νεώτερες εκδόσεις. Σε αυτές τις περιπτώσεις, θα δείτει μηνύματα όπως τα παρακάτω:

```
/usr/bin/ld: warning libz.so.4, needed by /usr/local/lib/libtiff.so, may conflict with
libz.so.5
/usr/bin/ld: warning: librpcsvc.so.4, needed by /usr/local/lib/libXext.so may conflict
with librpcsvc.so.5
```

Για να επιλύσετε τέτοιου είδους προβλήματα, βρείτε ποιο port εγκατέστησε την βιβλιοθήκη:

```
# pkg_info -W /usr/local/lib/libtiff.so
/usr/local/lib/libtiff.so was installed by package tiff-3.9.4
# pkg_info -W /usr/local/lib/libXext.so
/usr/local/lib/libXext.so was installed by package libXext-1.1.1,1
```

Έπειτα, απεγκαταστήστε, επαναμεταγλωττίστε και επανεγκατασήστε το port. Για να αυτοματοποιήσετε αυτή τη διαδικασία μπορείτε να χρησιμοποιήσετε τα βοηθητικά προγράμματα ports-mgmt/portmaster και ports-mgmt/portupgrade. Αφού βεβαιωθείτε ότι οι παλιές βιβλιοθήκες δεν χρησιμοποιούνται πλέον από κανένα πρόγραμμα, μπορείτε να τις διαγράψετε με την παρακάτω εντολή:

```
# make delete-old-libs
```

44.9. Διαδικασία για Πολλαπλά Μηχανήματα

Αν έχετε πολλαπλά μηχανήματα στα οποία πρόκειται να χρησιμοποιήσετε το ίδιο δέντρο πηγαίου κώδικα, είναι σπατάλη πόρων (δίσκου, δικτύου και επεξεργαστή) να επαναλαμβάνετε σε όλα τη διαδικασία ανάκτησης και μεταγλώττισης. Η λύση είναι να ορίσετε ένα μηχάνημα να εκτελεί το μεγαλύτερο μέρος της εργασίας, ενώ τα υπόλοιπα θα μπορούν να την ανακτούν μέσω NFS. Στην ενότητα αυτή θα παρουσιάσουμε ένα τρόπο με τον οποίο μπορεί να γίνει αυτό.

44.9.1. Προκαταρκτικά

Πρώτα από όλα, αναγνωρίστε το σετ των μηχανημάτων στα οποία σκοπεύετε να χρησιμοποιήσετε τα ίδια εκτελέσιμα. Θα ονομάσουμε αυτή την ομάδα *σετ μεταγλώττισης*. Κάθε μηχάνημα μπορεί να έχει δικό του προσαρμοσμένο πυρήνα, αλλά θα έχουν όλα τα ίδια εκτελέσιμα userland. Από το σετ αυτό, επιλέξτε ένα μηχάνημα το οποίο θα γίνει το *μηχάνημα μεταγλώττισης*. Θα είναι το μηχάνημα στο οποίο θα μεταγλωττίζεται το βασικό σύστημα και ο πυρήνας. Το ιδανικό είναι να επιλέξετε ένα γρήγορο μηχάνημα, στο οποίο να υπάρχει αρκετός ελεύθερος χρόνος στον επεξεργαστή για να εκτελεί τα `make buildworld` και `make buildkernel`. Θα πρέπει επίσης να επιλέξετε ένα *μηχάνημα δοκιμών* στο οποίο θα δοκιμάζετε τις ενημερώσεις λογισμικού πριν τις μεταφέρετε στην παραγωγή. Μπορεί να είναι και το ίδιο το μηχάνημα μεταγλώττισης, αλλά αυτό δεν είναι απαραίτητο.

Όλα τα μηχανήματα στο σετ μεταγλώττισης χρειάζεται να προσαρτήσουν το /usr/obj και το /usr/src

από το ίδιο μηχάνημα, και στο ίδιο σημείο προσάρτησης. Το ιδανικό είναι αυτά τα δύο συστήματα αρχείων να βρίσκονται σε διαφορετικό φυσικό δίσκο στο μηχάνημα μεταγλώττισης, αλλά μπορείτε να τα προσαρτήσετε μέσω NFS ακόμα και σε αυτό το μηχάνημα. Αν έχετε πολλαπλά σετ μεταγλώττισης, το /usr/src θα πρέπει να βρίσκεται σε ένα από τα μηχανήματα μεταγλώττισης, και να προσαρτάται στα υπόλοιπα μέσω NFS.

Τέλος, βεβαιωθείτε ότι τα αρχεία /etc/make.conf και /etc/src.conf σε όλα τα μηχανήματα του σετ μεταγλώττισης, είναι ίδια με τα αντίστοιχα στο μηχάνημα μεταγλώττισης. Αυτό σημαίνει ότι το μηχάνημα μεταγλώττισης θα πρέπει να μεταγλωττίζει όλα τα τμήματα του βασικού συστήματος τα οποία θα εγκατασταθούν σε κάθε μηχάνημα του σετ. Επίσης, σε κάθε μηχάνημα στο σετ μεταγλώττισης θα πρέπει να οριστεί το όνομα του δικού του προσαρμοσμένου πυρήνα μέσω της μεταβλητής `KERNCONF` στο /etc/make.conf, ενώ και το μηχάνημα μεταγλώττισης θα πρέπει να έχει μια λίστα όλων των άλλων στο `KERNCONF`, ξεκινώντας από το δικό του. Το μηχάνημα μεταγλώττισης, θα πρέπει να έχει τα αρχεία ρύθμισης του πυρήνα όλων των άλλων μηχανημάτων στον κατάλογο /usr/src/sys/arch/conf αν πρόκειται να μεταγλωττίζει τους πυρήνες τους.

44.9.2. Το Βασικό Σύστημα

Έχοντας πραγματοποιήσει όλα τα παραπάνω, είστε έτοιμος να μεταγλωττίσετε τα πάντα. Μεταγλωττίστε τον πυρήνα και το βασικό σύστημα όπως περιγράψαμε στο Μεταγλωττίστε το Βασικό Σύστημα χρησιμοποιώντας το μηχάνημα μεταγλώττισης, αλλά μην εγκαταστήσετε τίποτα. Μετά το τέλος της μεταγλώττισης, χρησιμοποιήστε το μηχάνημα δοκιμών και εγκαταστήστε τον πυρήνα που μόλις δημιουργήσατε. Αν το μηχάνημα αυτό προσαρτά το /usr/src και το /usr/obj μέσω NFS, όταν το επανεκκινήσετε σε κατάσταση ενός χρήστη, θα χρειαστεί να ενεργοποιήσετε το δίκτυο και να τα προσαρτήσετε. Ο ευκολότερος τρόπος για αυτό, είναι να εκκινήσετε σε κατάσταση πολλαπλών χρηστών και έπειτα να εκτελέσετε `shutdown now` για να μεταβείτε σε κατάσταση ενός χρήστη. Μόλις γίνει αυτό, μπορείτε να εγκαταστήσετε τον νέο πυρήνα και το βασικό σύστημα, και να εκτελέσετε το `mergemaster` όπως θα κάνατε συνήθως. Όταν τελειώσετε, επανεκκινήστε αυτό το μηχάνημα στην κανονική λειτουργία πολλαπλών χρηστών.

Όταν βεβαιωθείτε ότι όλα λειτουργούν σωστά στο μηχάνημα δοκιμών, χρησιμοποιήστε την ίδια διαδικασία για να εγκαταστήσετε το νέο λογισμικό σε κάθε ένα από τα υπόλοιπα μηχανήματα του σετ μεταγλώττισης.

44.9.3. Ports

Μπορείτε να χρησιμοποιήσετε τις ίδιες ιδέες και για το δέντρο των ports. Το πρώτο κρίσιμο βήμα είναι να προσαρτήσετε το /usr/ports από το ίδιο μηχάνημα, σε όλα τα μηχανήματα του σετ μεταγλώττισης. Μπορείτε έπειτα να ρυθμίσετε το /etc/make.conf ώστε να διαμοιράζονται τα distfiles. Θα πρέπει να θέσετε το `DISTDIR` σε ένα κοινόχρηστο κατάλογο, στον οποίο θα δώσετε δικαιώματα εγγραφής σε οποιοδήποτε χρήστη έχετε δηλώσει ως `root` στο NFS. Σε κάθε μηχάνημα θα πρέπει επίσης να οριστεί η μεταβλητή `WRKDIRPREFIX` ώστε να δείχνει σε ένα τοπικό κατάλογο. Τέλος, αν σκοπεύετε να μεταγλωττίζετε και να διανέμετε έτοιμα πακέτα, θα πρέπει να θέσετε την μεταβλητή `PACKAGES` σε ένα κατάλογο, όπως κάνατε και με την `DISTDIR`.

Chapter 45. DTrace

45.1. Σύνοψη

Το DTrace, γνωστό επίσης ως Dynamic Tracing, είναι ένα εργαλείο το οποίο αναπτύχθηκε από την Sun™ για τον εντοπισμό προβλημάτων απόδοσης σε συστήματα που πρόκειται να χρησιμοποιηθούν ή χρησιμοποιούνται ήδη στην παραγωγή. Δεν πρόκειται για εργαλείο αποσφαλμάτωσης, αλλά για εργαλείο ανάλυσης πραγματικού χρόνου, με το οποίο μπορούν να εντοπιστούν προβλήματα απόδοσης και άλλες καταστάσεις.

Το DTrace είναι ένα θαυμάσιο εργαλείο profiling και διαθέτει εντυπωσιακό πλήθος χαρακτηριστικών για την διάγνωση προβλημάτων του συστήματος. Μπορεί επίσης να χρησιμοποιηθεί για να εκτελέσει από πριν έτοιμα scripts, με τα οποία μπορείτε να εκμεταλλευθείτε καλύτερα τις δυνατότητες του. Οι χρήστες μπορούν ακόμα να γράψουν και τα δικά τους βοηθητικά προγράμματα, χρησιμοποιώντας την Γλώσσα D που παρέχει το DTrace, και να προσαρμόσουν με αυτό τον τρόπο το profiling στις δικές τους ανάγκες.

Αφού διαβάσετε αυτό το κεφάλαιο, θα γνωρίζετε:

- Τι είναι το DTrace και τι δυνατότητες παρέχει.
- Τις διαφορές υλοποίησης μεταξύ του DTrace του Solaris™ και του FreeBSD.
- Πως να ενεργοποιήσετε και να χρησιμοποιήσετε το DTrace στο FreeBSD.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε βασικές έννοιες του UNIX® και του FreeBSD (Βασικές Έννοιες στο UNIX®).
- Να είστε εξοικειωμένος με τις βασικές διαδικασίες ρύθμισης και μεταγλώττισης προσαρμοσμένου πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να είστε εξοικειωμένος με την ασφάλεια και τον τρόπο που αυτή σχετίζεται με το FreeBSD (Ασφάλεια).
- Να κατανοείτε πως μπορείτε να ανακτήσετε τον πηγαίο κώδικα του FreeBSD και να τον χρησιμοποιήσετε ώστε να επαναμεταγλωττίσετε το σύστημα σας (Ενημέρωση και Αναβάθμιση του FreeBSD).

Τη δεδομένη στιγμή, το DTrace θεωρείται ότι είναι σε πειραματικό στάδιο. Ορισμένες επιλογές μπορεί να υπολείπονται σε λειτουργικότητα, και κάποια τμήματα ίσως να μη λειτουργούν καθόλου. Με την πάροδο του χρόνου, οι παραπάνω δυνατότητες θα θεωρηθούν έτοιμες για χρήση σε μηχανήματα παραγωγής, και η παρούσα τεκμηρίωση θα ανανεωθεί ώστε να αντιπροσωπεύει αυτή την κατάσταση.

45.2. Διαφορές στην Υλοποίηση

Αν και το DTrace στο FreeBSD είναι αρκετά όμοιο με αυτό του Solaris™, υπάρχουν κάποιες διαφορές που θα πρέπει να τις εξηγήσουμε πριν συνεχίσουμε. Η μεγαλύτερη διαφορά που θα παρατηρήσουν

οι χρήστες, είναι ότι στο FreeBSD το DTrace πρέπει να ενεργοποιηθεί χειροκίνητα. Υπάρχουν διάφορες επιλογές και αρθρώματα για τον πυρήνα που πρέπει να ενεργοποιηθούν ώστε το DTrace να λειτουργεί σωστά. Θα εξηγήσουμε αργότερα αυτές τις ρυθμίσεις.

Η επιλογή `DDB_CTF` του πυρήνα χρησιμοποιείται για να ενεργοποιήσει την υποστήριξη φορτώματος των δεδομένων CTF από τον πυρήνα και τα αρθρώματα του. Το CTF είναι το Compact C Type format του Solaris™, το οποίο ενθυλακώνει μια ελαττωμένη μορφή πληροφοριών αποσφαλμάτωσης (debugging), όμοια με το DWARF και τα stabs. Αυτά τα δεδομένα CTF προστίθενται στα εκτελέσιμα μέσω των εργαλείων `ctfconvert` και `ctfmerge`. Το βοηθητικό πρόγραμμα `ctfconvert` ερμηνεύει τα τμήματα των DWARFELF που περιέχουν πληροφορίες debug (δημιουργούνται από το μεταγλωττιστή), και το `ctfmerge` συγχωνεύει τα τμήματα CTF και ELF από τα αντικείμενα σε άλλα εκτελέσιμα ή κοινόχρηστες βιβλιοθήκες. Περισσότερες πληροφορίες για την ενεργοποίηση των παραπάνω στη μεταγλώττιση του πυρήνα και του συστήματος του FreeBSD, θα δούμε παρακάτω.

Στο FreeBSD κάποιοι παροχείς είναι διαφορετικοί σε σχέση με το Solaris™. Ο πιο αξιοσημείωτος είναι ο παροχέας `dtmalloc` ο οποίος επιτρέπει το tracing του `malloc()` ανάλογα με τον τύπο του, στον πυρήνα του FreeBSD.

Μόνο ο `root` μπορεί να χρησιμοποιήσει το DTrace στο FreeBSD. Αυτό σχετίζεται με διαφορές στην ασφάλεια, καθώς το Solaris™ διαθέτει κάποιους ελέγχους ασφάλειας χαμηλού επιπέδου, οι οποίοι δεν υπάρχουν ακόμα στο FreeBSD. Για το λόγο αυτό, η χρήση της συσκευής /dev/dtrace/dtrace απαγορεύεται αυστηρά για όλους τους χρήστες εκτός από τον `root`.

Τέλος, το λογισμικό DTrace βρίσκεται υπό την άδεια CDDL της Sun™. Μπορείτε να διαβάσετε το κείμενο της άδειας `Common Development and Distribution License` στο FreeBSD, στο αρχείο /usr/src/cddl/contrib/opensolaris/OPENSOLARIS.LICENSE ή να το διαβάσετε online στη διεύθυνση http://www.opensolaris.org/os/licensing.

Η άδεια ουσιαστικά σημαίνει ότι ένας πυρήνας FreeBSD με τις επιλογές του DTrace, εξακολουθεί να βρίσκεται υπό την άδεια BSD. Ωστόσο το CDDL εμπλέκεται τη στιγμή που γίνεται διανομή των αρθρωμάτων σε δυαδική μορφή, ή τη στιγμή που φορτώνονται.

45.3. Ενεργοποίηση της Υποστήριξης DTrace

Για να ενεργοποιήσετε την υποστήριξη για το DTrace, προσθέστε τις ακόλουθες γραμμές στο αρχείο ρυθμίσεων του πυρήνα:

```
options         KDTRACE_HOOKS
options         DDB_CTF
```

Οι χρήστες της αρχιτεκτονικής AMD64 θα θέλουν να προσθέσουν την ακόλουθη γραμμή στο αρχείο ρυθμίσεων του πυρήνα τους:

```
options         KDTRACE_FRAME
```

Η επιλογή αυτή παρέχει υποστήριξη για τη λειτουργία FBT. Το DTrace μπορεί να λειτουργήσει και χωρίς αυτήν. Ωστόσο, θα παρέχει περιορισμένη υποστήριξη για

function boundary tracing.

Όλος ο πηγαίος κώδικας θα πρέπει να μεταγλωττιστεί ξανά με τις επιλογές CTF. Για να γίνει αυτό, μεταγλωττίστε ξανά το FreeBSD χρησιμοποιώντας:

```
# cd /usr/src

# make WITH_CTF=1 kernel
```

Θα χρειαστεί να επανεκκινήσετε το σύστημα.

Μετά την επανεκκίνηση, και με τον νέο πυρήνα φορτωμένο πλέον στη μνήμη, θα πρέπει να προσθέσετε υποστήριξη για το κέλυφος Korn. Αυτό απαιτείται, καθώς τα εργαλεία DTrace περιλαμβάνουν διάφορα βοηθητικά προγράμματα τα οποία είναι γραμμένα σε `ksh`. Εγκαταστήστε το port shells/ksh93. Μπορείτε επίσης να εκτελέσετε αυτά τα εργαλεία και μέσω του shells/pdksh ή του shells/mksh.

Τέλος, ανακτήστε την τρέχουσα σειρά εργαλείων DTrace. Η τελευταία έκδοση διατίθεται στην τοποθεσία http://www.opensolaris.org/os/community/dtrace/dtracetoolkit/. Διατίθεται και πρόγραμμα εγκατάστασης, το οποίο δεν είναι ωστόσο απαραίτητο να εκτελέσετε προκειμένου να χρησιμοποιήσετε τα εργαλεία.

45.4. Χρησιμοποιώντας το DTrace

Πριν χρησιμοποιήσετε τις λειτουργίες του DTrace, θα πρέπει να υπάρχει η αντίστοιχη συσκευή. Για να φορτώσετε τη συσκευή, θα πρέπει να δώσετε την παρακάτω εντολή:

```
# kldload dtraceall
```

Θα πρέπει να έχετε πλέον υποστήριξη DTrace. Για να δείτε όλα τα probes, θα πρέπει να εκτελέσετε ως διαχειριστής την παρακάτω εντολή:

```
# dtrace -l | more
```

Όλη η έξοδος περνάει μέσω του βοηθητικού προγράμματος `more`, διαφορετικά γρήγορα θα υπερχείλιζε την προσωρινή μνήμη της οθόνης. Στο σημείο αυτό, θα πρέπει να θεωρηθεί ότι το DTrace λειτουργεί. Είναι πλέον ώρα να εξετάσουμε αυτή τη σειρά εργαλείων.

Η σειρά των εργαλείων είναι μια συλλογή από έτοιμα scripts που εκτελούνται με το DTrace ώστε να συλλέξουν πληροφορίες σχετικά με το σύστημα. Υπάρχουν scripts που ελέγχουν για ανοικτά αρχεία, τη μνήμη, τη χρήση της CPU και πολλά ακόμα. Κάντε εξαγωγή των scripts με την ακόλουθη εντολή:

```
# gunzip -c DTraceToolkit* | tar xvf -
```

Μετακινηθείτε στον κατάλογο που τα αποσυμπιέσατε με την εντολή `cd` και αλλάξτε τα δικαιώματα

εκτέλεσης σε όλα τα αρχεία, όπως στα αρχεία με τα μικρά γράμματα, σε 755.

Θα χρειαστεί να γίνουν αλλαγές στο περιεχόμενο σε όλα τα scripts. Όσα περιέχουν το /usr/bin/ksh θα πρέπει να αλλαχθούν σε /usr/local/bin/ksh, τα άλλα που περιέχουν το /usr/bin/sh θα πρέπει να αλλαχθούν σε /bin/sh, και τέλος αυτά που περιέχουν το /usr/bin/perl θα πρέπει να αλλαχθούν σε /usr/local/bin/perl.

Στο σημείο αυτό είναι σημαντικό να υπενθυμίσουμε στον αναγνώστη ότι η υποστήριξη DTrace στο FreeBSD είναι *ατελής* και πειραματική. Πολλά από αυτά τα scripts δεν θα λειτουργήσουν, καθώς είναι είτε πολύ προσανατολισμένα στο Solaris™, ή χρησιμοποιούν probes τα οποία δεν υποστηρίζονται τη δεδομένη στιγμή.

Τη στιγμή που γράφονται αυτές οι γραμμές, μόνο δύο scripts από τη σειρά εργαλείων του DTrace υποστηρίζονται πλήρως στο FreeBSD: το hotkernel και το procsystime. Αυτά τα δύο θα εξερευνήσουμε στα επόμενα τμήματα αυτής της ενότητας.

Το hotkernel έχει σχεδιαστεί να αναγνωρίζει ποια συνάρτηση καταναλώνει το μεγαλύτερο χρόνο στον πυρήνα. Εκτελώντας το υπό κανονικές συνθήκες, θα δείτε έξοδο παρόμοια με την παρακάτω:

```
# ./hotkernel
Sampling... Hit Ctrl-C to end.
```

Ο διαχειριστής του συστήματος θα πρέπει να χρησιμοποιήσει το συνδυασμό πλήκτρων `Ctrl` + `C` για να σταματήσει τη διεργασία. Με τον τερματισμό του, το script θα απεικονίσει μια σειρά από συναρτήσεις του πυρήνα και πληροφορίες σχετικά με το χρόνο τους, ταξινομώντας τις σε αύξουσα σειρά ανάλογα με το χρόνο:

```
kernel`_thread_lock_flags                                 2   0.0%
0xc1097063                                                2   0.0%
kernel`sched_userret                                      2   0.0%
kernel`kern_select                                        2   0.0%
kernel`generic_copyin                                     3   0.0%
kernel`_mtx_assert                                        3   0.0%
kernel`vm_fault                                           3   0.0%
kernel`sopoll_generic                                     3   0.0%
kernel`fixup_filename                                     4   0.0%
kernel`_isitmyx                                           4   0.0%
kernel`find_instance                                      4   0.0%
kernel`_mtx_unlock_flags                                  5   0.0%
kernel`syscall                                            5   0.0%
kernel`DELAY                                              5   0.0%
0xc108a253                                                6   0.0%
kernel`witness_lock                                       7   0.0%
kernel`read_aux_data_no_wait                              7   0.0%
kernel`Xint0x80_syscall                                   7   0.0%
kernel`witness_checkorder                                 7   0.0%
kernel`sse2_pagezero                                      8   0.0%
```

```
kernel`strncmp                                          9   0.0%
kernel`spinlock_exit                                   10   0.0%
kernel`_mtx_lock_flags                                 11   0.0%
kernel`witness_unlock                                  15   0.0%
kernel`sched_idletd                                   137   0.3%
0xc10981a5                                          42139  99.3%
```

Το script αυτό λειτουργεί επίσης με αρθρώματα του πυρήνα. Για να χρησιμοποιήσετε αυτό το χαρακτηριστικό, εκτελέστε το με την επιλογή `-m`:

```
# ./hotkernel -m
Sampling... Hit Ctrl-C to end.
^C
MODULE                                                COUNT   PCNT
0xc107882e                                                1   0.0%
0xc10e6aa4                                                1   0.0%
0xc1076983                                                1   0.0%
0xc109708a                                                1   0.0%
0xc1075a5d                                                1   0.0%
0xc1077325                                                1   0.0%
0xc108a245                                                1   0.0%
0xc107730d                                                1   0.0%
0xc1097063                                                2   0.0%
0xc108a253                                               73   0.0%
kernel                                                  874   0.4%
0xc10981a5                                           213781  99.6%
```

Το procsystime script συλλαμβάνει και τυπώνει τον χρόνο των κλήσεων συστήματος για μια συγκεκριμένη διεργασία μέσω του PID ή του ονόματος της. Στο παρακάτω παράδειγμα έχουμε ξεκινήσει μια νέα διεργασία του /bin/csh. Εκτελέσαμε το procsystime και το αφήσαμε στην αναμονή καθώς γράφαμε μερικές εντολές στο `csh` που είχαμε ανοίξει. Αυτά είναι τα αποτελέσματα της δοκιμής μας:

```
# ./procsystime -n csh
Tracing... Hit Ctrl-C to end...
^C

Elapsed Times for processes csh,

         SYSCALL          TIME (ns)
          getpid               6131
       sigreturn               8121
           close              19127
           fcntl              19959
             dup              26955
         setpgid              28070
            stat              31899
       setitimer              40938
```

```
           wait4               62717
       sigaction               67372
     sigprocmask              119091
    gettimeofday              183710
           write              263242
          execve              492547
           ioctl              770073
           vfork             3258923
      sigsuspend             6985124
            read          3988049784
```

Όπως φαίνεται, η κλήση του συστήματος για ανάγνωση (`read()`) είναι αυτή που καταναλώνει τον περισσότερο χρόνο σε νανοδευτερόλεπτα, ενώ το λιγότερο τον καταναλώνει η κλήση συστήματος `getpid()`.

45.5. Η Γλώσσα D

Η σειρά εργαλείων DTrace, περιλαμβάνει αρκετά scripts γραμμένα στην ειδική γλώσσα του DTrace. Η γλώσσα αυτή ονομάζεται "η γλώσσα D" στην τεκμηρίωση της Sun™, και είναι αρκετά όμοια με τη C++. Αναλυτική περιγραφή αυτής της γλώσσας είναι πέρα από τους σκοπούς αυτού του κειμένου. Υπάρχει ενεργή συζήτηση σχετικά με αυτή, στη διεύθυνση http://wikis.sun.com/display/DTrace/Documentation.

params: path: "/books/handbook/partiv/" :leveloffset: +1

Part IV: Serial Communications

Chapter 46. Σύνοψη

Το UNIX® πάντοτε υποστήριζε σειριακές επικοινωνίες. Για την ακρίβεια, τα πρώτα UNIX® μηχανήματα βασίζονταν σε σειριακές γραμμές για την είσοδο και έξοδο στο χρήστη. Τα πράγματα ωστόσο έχουν αλλάξει πολύ από τις μέρες που το συνηθισμένο "τερματικό" αποτελούνταν από ένα σειριακό εκτυπωτή 10 χαρακτήρων το δευτερόλεπτο και ένα πληκτρολόγιο. Το κεφάλαιο αυτό θα καλύψει κάποιους από τους τρόπους σειριακής επικοινωνίας που χρησιμοποιούνται από το FreeBSD.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να συνδέσετε τερματικά στο FreeBSD σύστημα σας.
- Πως να χρησιμοποιήσετε ένα modem για να συνδεθείτε σε απομακρυσμένα συστήματα.
- Πως να επιτρέψετε σε απομακρυσμένους χρήστες να συνδεθούν στο σύστημα σας μέσω modem.
- Πως να εκκινήσετε το σύστημα σας μέσω σειριακής κονσόλας.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ξέρετε πως θα ρυθμίσετε και θα εγκαταστήσετε ένα νέο πυρήνα (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να κατανοείτε τις άδειες και διεργασίες του UNIX® (Βασικές Έννοιες στο UNIX®).
- Να έχετε πρόσβαση στο τεχνικό εγχειρίδιο του υλικού σας (modem ή κάρτα πολλαπλών σειριακών θυρών) που θέλετε να χρησιμοποιήσετε στο FreeBSD.

Chapter 47. Εισαγωγή

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών των σειριακών θυρών μετονομάστηκαν από /dev/cuadN σε /dev/cuauN και από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την παρακάτω τεκμηρίωση σύμφωνα με τις παραπάνω αλλαγές.

47.1. Ορολογία

bps

Bits Ανά Δευτερόλεπτο - ο ρυθμός μετάδοσης των δεδομένων

DTE

Data Terminal Equipment, Τερματικός Εξοπλισμός Δεδομένων - για παράδειγμα, ο υπολογιστής σας

DCE

Data Communications Equipment, Εξοπλισμός Επικοινωνίας Δεδομένων - το modem σας

RS-232

Πρότυπο της EIA για το υλικό που χρησιμοποιείται στις σειριακές επικοινωνίες

Όταν αναφερόμαστε στο ρυθμό μετάδοσης δεδομένων επικοινωνίας, δεν χρησιμοποιούμε πάντοτε τον όρο "baud". Το baud αναφέρεται στον αριθμό των μεταβάσεων του ηλεκτρικού σήματος στη μονάδα του χρόνου, ενώ κανονικά πρέπει να χρησιμοποιείται το "bps" (bits ανά δευτερόλεπτο) που είναι ο *σωστός* όρος (η τουλάχιστον δεν φαίνεται να ενοχλεί πολύ τους σχολαστικούς).

47.2. Θύρες και Καλώδια

Για να συνδέσετε ένα modem ή τερματικό στο FreeBSD σύστημα σας, θα χρειαστείτε μια σειριακή θύρα στον υπολογιστή σας, και το κατάλληλο καλώδιο για να συνδέσετε τη σειριακή συσκευή σας. Αν είστε ήδη εξοικειωμένος με το υλικό σας και το καλώδιο που απαιτείται, μπορείτε με ασφάλεια να παραλείψετε αυτή την ενότητα.

47.2.1. Καλώδια

Υπάρχουν αρκετοί διαφορετικοί τύποι σειριακών καλωδίων. Οι δύο πιο κοινοί τύποι για τους σκοπούς μας, είναι τα καλώδια τύπου null-modem και τα τυποποιημένα καλώδια RS-232 (γνωστά και ως "ευθείες"). Η τεκμηρίωση του υλικού σας θα πρέπει να περιγράφει τον τύπο του καλωδίου που απαιτείται.

47.2.1.1. Καλώδια Τύπου Null-modem

Ένα καλώδιο τύπου null-modem, μεταφέρει απευθείας κάποια σήματα όπως η "Γείωση Σήματος (SG)", αλλά αντιστρέφει τις συνδέσεις σε κάποια άλλα. Για παράδειγμα, ο ακροδέκτης "Μετάδοσης Δεδομένων" (γνωστός και ως TD) της μιας πλευράς, συνδέεται με τον ακροδέκτη "Λήψης Δεδομένων" (γνωστός και ως RD) της άλλης.

Μπορείτε επίσης να φτιάξετε το δικό σας καλώδιο τύπου null-modem (π.χ. για λόγους ποιότητας) για χρήση με τερματικά. Ο παρακάτω πίνακας δείχνει τα σήματα του RS-232 και τους αριθμούς των ακροδεκτών σε ένα συνδέτη DB-25. Σημειώστε επίσης ότι το πρότυπο ορίζει απευθείας σύνδεση των ακροδεκτών 1 της κάθε άκρης. Πρόκειται για τον ακροδέκτη της *Προστατευτικής Γείωσης*, αλλά συχνά η σύνδεση του παραλείπεται. Μερικά τερματικά λειτουργούν κανονικά χρησιμοποιώντας μόνο τους ακροδέκτες 2, 3 και 7, ενώ κάποιοι άλλα απαιτούν διαφορετικές ρυθμίσεις σε σχέση με τα παραδείγματα που φαίνονται παρακάτω.

Πίνακας 4. Καλώδιο Null-Modem DB-25 σε DB-25

Σήμα	Ακροδέκτης #		Ακροδέκτης #	Σήμα
SG	7	συνδέεται στο	7	SG
TD	2	συνδέεται στο	3	RD
RD	3	συνδέεται στο	2	TD
RTS	4	συνδέεται στο	5	CTS
CTS	5	συνδέεται στο	4	RTS
DTR	20	συνδέεται στο	6	DSR
DTR	20	συνδέεται στο	8	DCD
DSR	6	συνδέεται στο	20	DTR
DCD	8	συνδέεται στο	20	DTR

Παρακάτω φαίνονται δύο διατάξεις που είναι πιο κοινές στις μέρες μας.

Πίνακας 5. Καλώδιο Null-Modem DB-9 σε DB-9

Σήμα	Ακροδέκτης #		Ακροδέκτης #	Σήμα
RD	2	συνδέεται στο	3	TD
TD	3	συνδέεται στο	2	RD
DTR	4	συνδέεται στο	6	DSR
DTR	4	συνδέεται στο	1	DCD
SG	5	συνδέεται στο	5	SG
DSR	6	συνδέεται στο	4	DTR
DCD	1	συνδέεται στο	4	DTR
RTS	7	συνδέεται στο	8	CTS
CTS	8	συνδέεται στο	7	RTS

Πίνακας 6. Καλώδιο Null-Modem DB-9 σε DB-25

Σήμα	Ακροδέκτης #		Ακροδέκτης #	Σήμα
RD	2	συνδέεται στο	2	TD
TD	3	συνδέεται στο	3	RD
DTR	4	συνδέεται στο	6	DSR

Σήμα	Ακροδέκτης #		Ακροδέκτης #	Σήμα
DTR	4	συνδέεται στο	8	DCD
SG	5	συνδέεται στο	7	SG
DSR	6	συνδέεται στο	20	DTR
DCD	1	συνδέεται στο	20	DTR
RTS	7	συνδέεται στο	5	CTS
CTS	8	συνδέεται στο	4	RTS

Όταν ένας ακροδέκτης σε μια άκρη χρειάζεται να συνδεθεί με δύο ακροδέκτες στην άλλη, συνήθως ενώνουμε τους ακροδέκτες μεταξύ τους στη μια άκρη με ένα μικρό καλώδιο, και χρησιμοποιούμε ένα μακρύτερο καλώδιο για την ένωση με την άλλη άκρη.

Η παραπάνω διάταξη φαίνεται να είναι η πιο διαδεδομένη. Σε μια παραλλαγή (που εξηγείται στο βιβλίο *Το RS-232 με Απλά Βήματα*), το SG συνδέεται στο SG, το TD συνδέεται στο RD, τα RTS και CTS συνδέονται στο DCD, το DTR συνδέεται στο DSR, και αντίστροφα.

47.2.1.2. Τυποποιημένα Καλώδια RS-232C

Ένα τυποποιημένο σειριακό καλώδιο RS-232C, μεταφέρει όλα τα σήματα απευθείας από τη μια άκρη στην άλλη, χωρίς καμιά αλλαγή στους ακροδέκτες. Αυτό απλά σημαίνει ότι ο ακροδέκτης "Μετάδοσης Δεδομένων (TD)" της μιας άκρης, συνδέεται στον ακροδέκτη "Μετάδοσης Δεδομένων (TD)" της άλλης άκρης. Αυτό είναι και το είδος του καλωδίου που θα χρησιμοποιήσετε για να συνδέσετε ένα modem στο FreeBSD σύστημα σας, και είναι επίσης κατάλληλο για ορισμένα τερματικά.

47.2.2. Θύρες

Οι σειριακές θύρες είναι οι συσκευές που μεταφέρουν τα δεδομένα μεταξύ του FreeBSD συστήματος και του τερματικού. Η ενότητα αυτή περιγράφει τα είδη των θυρών που υπάρχουν, και πως τα χειρίζεται το FreeBSD.

47.2.2.1. Είδη Θυρών

Υπάρχουν διάφορα είδη σειριακών θυρών. Πριν αγοράσετε ή κατασκευάσετε κάποιο καλώδιο, θα πρέπει να βεβαιωθείτε ότι ταιριάζει με τη θύρα του τερματικού και του FreeBSD συστήματος σας.

Τα περισσότερα τερματικά διαθέτουν θύρες DB-25. Οι προσωπικοί υπολογιστές, συμπεριλαμβανομένων και αυτών που εκτελούν FreeBSD, μπορεί να έχουν θύρες τύπου DB-25 ή DB-9. Αν διαθέτετε κάρτα πολλαπλών σειριακών θυρών στον υπολογιστή σας, μπορεί να διαθέτει θύρες τύπου RJ-12 ή RJ-45.

Δείτε την τεκμηρίωση που συνοδεύει το υλικό σας, για τις τεχνικές προδιαγραφές της θύρας που χρησιμοποιεί. Συνήθως μπορείτε να βγάλετε συμπέρασμα αν απλώς κοιτάξετε την υποδοχή.

47.2.2.2. Ονόματα Θυρών

Στο FreeBSD, έχετε πρόσβαση σε κάθε σειριακή θύρα μέσω μιας καταχώρισης στον κατάλογο /dev. Υπάρχουν δύο διαφορετικά είδη καταχωρίσεων:

- Οι θύρες που μπορούν να χρησιμοποιηθούν για είσοδο στο σύστημα, ονομάζονται /dev/ttyuN όπου το *N* είναι ο αριθμός της θύρας (η αρίθμηση ξεκινάει από το μηδέν). Γενικά, οι θύρες αυτές προορίζονται για σύνδεση με τερματικά. Οι θύρες εισόδου απαιτούν να είναι ενεργό το σήμα ανίχνευσης φέροντος (DCD) στη σειριακή γραμμή, προκειμένου να λειτουργήσουν σωστά.
- Οι θύρες κλήσης ή εξόδου, ονομάζονται /dev/cuauN. Οι θύρες αυτές δεν χρησιμοποιούνται συνήθως για τερματικά, αλλά για modems. Μπορείτε να χρησιμοποιήσετε αυτή τη θύρα για κάποιο τερματικό που δεν υποστηρίζει το σήμα ανίχνευσης φέροντος.

Αν έχετε συνδέσει ένα τερματικό στην πρώτη σειριακή θύρα (που στο MS-DOS® αναφέρεται ως COM1), θα πρέπει να χρησιμοποιήσετε την συσκευή /dev/ttyu0 για να αναφερθείτε στο τερματικό. Αν το τερματικό είναι στη δεύτερη σειριακή θύρα (που είναι επίσης γνωστή ως COM2) χρησιμοποιήστε τη συσκευή /dev/ttyu1, κ.ο.κ.

47.3. Ρύθμιση του Πυρήνα

Το FreeBSD από προεπιλογή υποστηρίζει τέσσερις σειριακές θύρες. Στον κόσμο του MS-DOS® οι θύρες αυτές είναι γνωστές ως: COM1, COM2, COM3, και COM4. Το FreeBSD αυτή τη στιγμή υποστηρίζει "κουτές" σειριακές κάρτες πολλαπλών θυρών, όπως τις BocaBoard 1008 και 2016, όπως και πιο ευφυής κάρτες, όπως αυτές που κατασκευάζονται από την Digiboard και την Stallion Technologies. Ο προεπιλεγμένος πυρήνας ωστόσο, εκτελεί ανίχνευση μόνο για τις τυπικές σειριακές (COM) θύρες.

Για να δείτε αν ο πυρήνας σας αναγνωρίζει οποιαδήποτε από τις σειριακές θύρες, παρατηρήστε τα μηνύματα κατά τη διάρκεια εκκίνησης του συστήματος, ή χρησιμοποιήστε την εντολή `/sbin/dmesg` για να ξαναδείτε τα μηνύματα του πυρήνα κατά τη διάρκεια της εκκίνησης. Πιο συγκεκριμένα, αναζητήστε τα μηνύματα που ξεκινούν με τους χαρακτήρες `sio`.

Για να δείτε μόνο τα μηνύματα που περιέχουν τη λέξη `sio`, χρησιμοποιήστε την εντολή:

```
# /sbin/dmesg | grep 'sio'
```

Για παράδειγμα, σε ένα σύστημα με τέσσερις σειριακές θύρες, τα μηνύματα του πυρήνα που σχετίζονται με αυτές φαίνονται παρακάτω:

```
sio0 at 0x3f8-0x3ff irq 4 on isa
sio0: type 16550A
sio1 at 0x2f8-0x2ff irq 3 on isa
sio1: type 16550A
sio2 at 0x3e8-0x3ef irq 5 on isa
sio2: type 16550A
sio3 at 0x2e8-0x2ef irq 9 on isa
```

```
sio3: type 16550A
```

Αν ο πυρήνας σας δεν αναγνωρίζει όλες τις σειριακές σας θύρες, πιθανόν να χρειαστεί να τον ρυθμίσετε χρησιμοποιώντας το αρχείο /boot/device.hints. Μπορείτε επίσης να μετατρέψετε σε σχόλιο (ή και να διαγράψετε τελείως) γραμμές που αναφέρονται σε συσκευές που δεν υπάρχουν στο σύστημα σας.

Παρακαλούμε ανατρέξτε στη σελίδα manual του sio(4) για περισσότερες πληροφορίες σχετικά με τις σειριακές θύρες και τις ρυθμίσεις των καρτών πολλαπλών σειριακών θυρών. Αν χρησιμοποιείτε αρχείο ρυθμίσεων που προέρχεται από κάποια παλαιότερη έκδοση του FreeBSD, θα πρέπει να είστε ιδιαίτερα προσεκτικοί, καθώς κάποιες από τις επιλογές των συσκευών και η σύνταξη τους έχουν αλλάξει στις νεότερες εκδόσεις.

Το `port IO_COM1` υποκαθιστά το `port 0x3f8`, `IO_COM2` είναι το `0x2f8`, `IO_COM3` είναι το `0x3e8`, και το `IO_COM4` είναι το `0x2e8`. Αυτές είναι και οι πιο κοινές ρυθμίσεις για τις παραπάνω θύρες. Οι γραμμές interrupt 4, 3, 5 και 9 είναι οι πλέον συνηθισμένες στις σειριακές θύρες. Σημειώστε επίσης ότι οι συνηθισμένες σειριακές θύρες *δεν* μπορούν να μοιράζονται το ίδιο interrupt με κάποια άλλη συσκευή σε υπολογιστές που διαθέτουν δίαυλο τύπου ISA (οι κάρτες πολλαπλών θυρών διαθέτουν ειδικά κυκλώματα που επιτρέπουν σε όλα τα 16550A που χρησιμοποιεί η κάρτα να λειτουργούν χρησιμοποιώντας μόνο μία ή δύο γραμμές interrupt).

47.4. Ειδικά Αρχεία Συσκευών

Η πρόσβαση στις περισσότερες συσκευές του πυρήνα, επιτυγχάνεται μέσω "ειδικών αρχείων συσκευών", τα οποία βρίσκονται στον κατάλογο /dev/. Στις συσκευές sio η πρόσβαση επιτυγχάνεται μέσω των αρχείων /dev/ttyuN (για συσκευές εισόδου, dial-in) και /dev/cuauN (για συσκευές εξόδου, call-out). Το FreeBSD παρέχει επίσης συσκευές αρχικοποίησης (/dev/ttyuN.init και /dev/cuauN.init) και συσκευές κλειδώματος (/dev/ttyuN.lock και /dev/cuauN.lock). Οι συσκευές αρχικοποίησης χρησιμοποιούνται για την ρύθμιση των αρχικών παραμέτρων επικοινωνίας στη θύρα, κάθε φορά που ανοίγει. Τέτοιες παράμετροι είναι π.χ. το `crtscts` για τα modems που χρησιμοποιούν σηματοδοσία `RTS/CTS` για έλεγχο ροής. Οι συσκευές κλειδώματος χρησιμοποιούνται για να κλειδώνουν κάποιες ρυθμίσεις στις θύρες, ώστε να μην μπορούν να αλλαχθούν από άλλους χρήστες ή προγράμματα. Για πληροφορίες σχετικές με τις ρυθμίσεις τερματικών, την αρχικοποίηση και τα κλειδώματα συσκευών, και τη ρύθμιση παραμέτρων στα τερματικά, δείτε αντίστοιχα τις σελίδες manual termios(4), sio(4), και stty(1).

47.5. Ρυθμίσεις Σειριακών Θυρών

Η συσκευή ttyuN (ή cuauN) είναι η κανονική συσκευή που μπορείτε να χρησιμοποιήσετε στις εφαρμογές σας. Όταν μια διαδικασία ανοίγει μια συσκευή, χρησιμοποιούνται κάποιες προεπιλεγμένες ρυθμίσεις I/O για το τερματικό. Μπορείτε να δείτε αυτές τις ρυθμίσεις με την εντολή:

```
# stty -a -f /dev/ttyu1
```

Αν αλλάξετε τις ρυθμίσεις σε αυτή τη συσκευή, αυτές θα παραμείνουν μέχρι το κλείσιμο της συσκευής. Όταν ανοιχθεί ξανά, θα έχει επανέλθει στις προεπιλεγμένες ρυθμίσεις. Για να αλλάξετε τις προεπιλεγμένες ρυθμίσεις, μπορείτε να ανοίξετε και να αλλάξετε τις ρυθμίσεις της συσκευής "αρχικής κατάστασης". Για παράδειγμα, για να ενεργοποιήσετε τη λειτουργία `CLOCAL`, να ορίσετε επικοινωνία 8bit και έλεγχο ροής μέσω `XON/XOFF` για τη συσκευή ttyu5, γράψτε:

```
# stty -f /dev/ttyu5.init clocal cs8 ixon ixoff
```

Η αρχικοποίηση των σειριακών συσκευών για όλο το σύστημα, ελέγχεται από το αρχείο /etc/rc.d/serial. Το αρχείο αυτό επηρεάζει τις προεπιλεγμένες ρυθμίσεις των σειριακών συσκευών.

Για να αποτρέψετε την αλλαγή συγκεκριμένων ρυθμίσεων από κάποια εφαρμογή, αλλάξτε τις ρυθμίσεις της συσκευής "κλειδώματος". Για παράδειγμα, για να κλειδώσετε την ταχύτητα της συσκευής ttyu5 στα 57600 bps, γράψτε:

```
# stty -f /dev/ttyu5.lock 57600
```

Τώρα, μια εφαρμογή που ανοίγει τη θύρα ttyu5 και επιχειρεί να αλλάξει την ταχύτητα της θύρας, θα αναγκαστεί να παραμείνει στα 57600 bps.

Φυσικά, θα πρέπει να ρυθμίσετε τις συσκευές αρχικοποίησης και κλειδώματος, ώστε να είναι εγγράψιμες μόνο από τον λογαριασμό του `root`.

Chapter 48. Τερματικά

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών των σειριακών θυρών μετονομάστηκαν από /dev/cuadN σε /dev/cuauN και από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την παρακάτω τεκμηρίωση σύμφωνα με τις παραπάνω αλλαγές.

Τα τερματικά παρέχουν μια βολική και χαμηλού κόστους μέθοδο πρόσβασης στο FreeBSD σύστημα σας, όταν δεν βρίσκεστε μπροστά στην κονσόλα ή σε κάποιο συνδεμένο δίκτυο. Η ενότητα αυτή περιγράφει πως να χρησιμοποιήσετε τερματικά στο FreeBSD.

48.1. Χρήσεις και Είδη Τερματικών

Τα αρχικά συστήματα UNIX® δεν είχαν κονσόλες. Αντίθετα, οι χρήστες εισέρχονταν στο σύστημα και εκτελούσαν τα προγράμματα τους μέσω τερματικών που συνδέονταν στις σειριακές θύρες του υπολογιστή. Αυτό μοιάζει αρκετά με τη χρήση modem και λογισμικού εξομοίωσης τερματικού για σύνδεση σε ένα απομακρυσμένο σύστημα. Με τον τρόπο αυτό μπορείτε βέβαια να εκτελέσετε εργασίες μόνο σε περιβάλλον κειμένου.

Τα σημερινά PC διαθέτουν κονσόλες ικανές να απεικονίσουν γραφικά πολύ υψηλής ποιότητας, αλλά η ικανότητα σύνδεσης στο μηχάνημα μέσω σειριακής θύρας, υπάρχει ακόμα σχεδόν σε όλα τα σημερινά συστήματα τύπου UNIX®. Το FreeBSD δεν αποτελεί εξαίρεση. Συνδέοντας ένα τερματικό σε μια αχρησιμοποίητη σειριακή θύρα, μπορείτε να εισέλθετε στο σύστημα και να εκτελέσετε οποιοδήποτε πρόγραμμα κειμένου το οποίο θα μπορούσατε φυσιολογικά να εκτελέσετε στην κονσόλα ή σε ένα παράθυρο `xterm` του συστήματος X Window.

Για χρήση σε επιχειρήσεις, είναι δυνατόν να συνδέσετε πολλά τερματικά σε ένα FreeBSD σύστημα και να τα τοποθετήσετε στις θέσεις εργασίας των υπαλλήλων. Ένας οικιακός χρήστης μπορεί να χρησιμοποιήσει κάποιο παλιό υπολογιστή (π.χ. ένα παλιό IBM PC ή Macintosh®) ως τερματικό ενός πολύ ισχυρότερου υπολογιστή που εκτελεί FreeBSD. Με τον τρόπο αυτό, μπορείτε να μετατρέψετε αυτό που κανονικά θα ήταν σύστημα ενός χρήστη, σε ένα πανίσχυρο σύστημα πολλαπλών χρηστών.

Στο FreeBSD υπάρχουν τρία είδη τερματικών:

- Κουτά Τερματικά
- PC που λειτουργούν ως τερματικά
- Τερματικά X

Οι παρακάτω υποενότητες περιγράφουν καθένα από αυτούς τους τύπους.

48.1.1. Κουτά Τερματικά

Τα κουτά τερματικά είναι εξειδικευμένες συσκευές που επιτρέπουν τη σύνδεση σε υπολογιστές μέσω σειριακών γραμμών. Αποκαλούνται "κουτά" ακριβώς επειδή η μόνη υπολογιστική ισχύ που έχουν είναι για απεικόνιση, αποστολή, και λήψη κειμένου. Δεν μπορείτε να εκτελέσετε προγράμματα σε αυτά. Όλη η ισχύς τους προέρχεται από τον υπολογιστή που θα τα συνδέσετε, και μέσω αυτού μπορείτε να εκτελέσετε συντάκτες κειμένου, μεταγλωττιστές, προγράμματα email,

παιχνίδια κ.ο.κ.

Υπάρχουν εκατοντάδες είδη κουτών τερματικών από αρκετούς κατασκευαστές, όπως το VT-100 της Digital Equipment Corporation και το WY-75 της Wyse. Σχεδόν οποιοσδήποτε τύπος μπορεί να λειτουργήσει με το FreeBSD. Μερικά τερματικά υψηλού κόστους μπορούν επίσης να απεικονίσουν και γραφικά, αλλά αυτή τη δυνατότητα μπορούν να την εκμεταλλευθούν σχετικά λίγα πακέτα λογισμικού.

Τα κουτά τερματικά είναι δημοφιλή σε περιβάλλοντα εργασίας όπου οι εργαζόμενοι δεν χρειάζονται πρόσβαση σε γραφικές εφαρμογές, όπως αυτές που παρέχονται από το σύστημα X Window.

48.1.2. PC που Λειτουργούν ως Τερματικά

Αν ένα κουτό τερματικό έχει ακριβώς την ισχύ που χρειάζεται για να δείχνει, να στέλνει, και να λαμβάνει κείμενο, τότε και κάθε υπολογιστής που σας περισσεύει μπορεί να λειτουργήσει σαν κουτό τερματικό. Το μόνο που χρειάζεστε είναι το σωστό καλώδιο και κάποιο πρόγραμμα *εξομοίωσης τερματικού* το οποίο θα εκτελείτε στον υπολογιστή αυτό.

Η παραπάνω διάταξη είναι δημοφιλής για οικιακή χρήση. Αν για παράδειγμα κάποιος δουλεύει στην κονσόλα του συστήματος σας, μπορείτε να εκτελέσετε την εργασία σας (με την προϋπόθεσή ότι είναι μόνο κείμενο) την ίδια στιγμή, χρησιμοποιώντας ένα λιγότερο ισχυρό σύστημα το οποίο συνδέεται στο FreeBSD σας ως τερματικό.

Υπάρχουν δύο τουλάχιστον βοηθητικά προγράμματα στο βασικό σύστημα του FreeBSD που μπορούν να χρησιμοποιηθούν για να δουλέψετε μέσω σειριακής σύνδεσης: το cu(1) και το tip(1).

Για να συνδεθείτε από ένα άλλο μηχάνημα που εκτελεί FreeBSD στη σειριακή σύνδεση ενός άλλου συστήματος, μπορείτε να χρησιμοποιήσετε την παρακάτω εντολή:

```
# cu -l serial-port-device
```

Όπου το "serial-port-device" είναι το όνομα του αρχείου συσκευής που αντιπροσωπεύει μια σειριακή θύρα στο σύστημα σας. Αυτά τα αρχεία συσκευών καλούνται /dev/cuauN.

Το "N" στο όνομα της συσκευής, αντιπροσωπεύει τον αριθμό της σειριακής θύρας.

Σημειώστε ότι η αρίθμηση των συσκευών στο FreeBSD ξεκινά από το μηδέν, και όχι από το ένα (όπως συμβαίνει για παράδειγμα στα συστήματα που σχετίζονται με το MS-DOS®). Αυτό πρακτικά σημαίνει ότι η θύρα που στο MS-DOS® καλείται COM1 θα είναι συνήθως η /dev/cuau0 στο FreeBSD.

Κάποιοι χρήστες προτιμούν να χρησιμοποιούν άλλα προγράμματα που διατίθενται μέσω της Συλλογής των Ports. Τα Ports περιλαμβάνουν αρκετά βοηθητικά προγράμματα με λειτουργίες παρόμοιες με το cu(1) και το tip(1), για παράδειγμα το comms/minicom.

48.1.3. Τερματικά X

Τα τερματικά X είναι τα πιο εξελιγμένα είδη τερματικών που υπάρχουν. Αντί να συνδέονται σε σειριακή θύρα, συνήθως συνδέονται μέσω δικτύου, π.χ. Ethernet. Αντί να περιορίζονται μόνο σε εφαρμογές κειμένου, μπορούν να απεικονίσουν οποιαδήποτε εφαρμογή των X.

Αναφέραμε τα τερματικά X μόνο για λόγους πληρότητας αυτής της ενότητας. Στο κεφάλαιο αυτό ωστόσο, *δεν* καλύπτεται η εγκατάσταση, ρύθμιση, και χρήση των τερματικών X.

48.2. Ρύθμιση

Η ενότητα αυτή περιγράφει τι χρειάζεται να ρυθμίσετε στο FreeBSD σύστημα σας για να είναι δυνατή η είσοδος σε αυτό μέσω τερματικού. Προϋποθέτει ότι έχετε ήδη ρυθμίσει τον πυρήνα σας να υποστηρίζει τη σειριακή θύρα στην οποία είναι συνδεμένη το τερματικό-και ότι το έχετε ήδη συνδέσει.

Στο Η Διαδικασία Εκκίνησης του FreeBSD είδαμε ότι η διεργασία `init` είναι υπεύθυνη για τον έλεγχο των άλλων διεργασιών, και για την αρχικοποίηση κατά την εκκίνηση του συστήματος. Μια από τις εργασίες που εκτελεί η `init` είναι να διαβάζει το αρχείο /etc/ttys και να ξεκινά μια διεργασία `getty` σε κάθε διαθέσιμο τερματικό. Η διεργασία `getty` αναλαμβάνει να διαβάσει το όνομα χρήστη και να ξεκινήσει το πρόγραμμα `login`.

Για να ρυθμιστούν τα τερματικά στο FreeBSD σύστημα σας, θα πρέπει να εκτελέσετε τα ακόλουθα βήματα ως `root`:

1. Προσθέστε μια γραμμή στο /etc/ttys με το όνομα της συσκευής όπως φαίνεται στον κατάλογο /dev, αν δεν υπάρχει ήδη.
2. Καθορίστε ότι θα εκτελείται η `/usr/libexec/getty` στην θύρα, και επιλέξτε τον κατάλληλο τύπο *getty* από το αρχείο /etc/gettytab.
3. Καθορίστε τον προεπιλεγμένο τύπο τερματικού.
4. Ενεργοποιήστε τη θύρα θέτοντας την αντίστοιχη επιλογή στο "on".
5. Επιλέξτε αν η θύρα θα είναι ασφαλής με την επιλογή "secure".
6. Εξαναγκάστε την `init` να διαβάσει ξανά το αρχείο /etc/ttys.

Ως προαιρετικό βήμα, μπορείτε να δημιουργήσετε ένα προσαρμοσμένο τύπο *getty* για να τον χρησιμοποιήσετε στο βήμα 2, στην καταχώριση του /etc/gettytab. Στο κεφάλαιο αυτό δεν θα σας εξηγήσουμε πως γίνεται αυτό. Σας προτρέπουμε να διαβάσετε τις σελίδες manual του gettytab(5) και getty(8) για περισσότερες πληροφορίες.

48.2.1. Προσθέτοντας μια Καταχώριση στο /etc/ttys

Το αρχείο /etc/ttys περιέχει μια λίστα όλων των θυρών του FreeBSD συστήματος σας στις οποίες θέλετε να επιτρέπεται η είσοδος στο σύστημα. Για παράδειγμα, υπάρχει μια καταχώριση σε αυτό το αρχείο για την πρώτη εικονική κονσόλα ttyv0. Μέσω αυτής της καταχώρισης, μπορείτε να εισέλθετε στο σύστημα από την κονσόλα. Το αρχείο αυτό περιέχει επίσης καταχωρίσεις για άλλες εικονικές κονσόλες, σειριακές θύρες και ψευδό-τερματικά. Για κάποιο τερματικό που είναι συνδεμένο απευθείας σε μια σειριακή θύρα, γράψτε απλώς την καταχώριση της σειριακής συσκευής όπως

φαίνεται στον κατάλογο /dev, χωρίς να γράψετε και τον κατάλογο /dev (για παράδειγμα, η συσκευή /dev/ttyv0 θα καταχωρισθεί ως ttyv0).

Η προεπιλεγμένη εγκατάσταση του FreeBSD περιέχει ένα αρχείο /etc/ttys το οποίο υποστηρίζει τις πρώτες τέσσερις σειριακές θύρες: ttyu0 ως και ttyu3. Αν συνδέσετε τερματικό σε κάποια από αυτές τις θύρες, δεν χρειάζεται να προσθέσετε άλλη καταχώριση.

Παράδειγμα 20. Προσθήκη Καταχωρίσεων για τα Τερματικά στο /etc/ttys

Ας υποθέσουμε ότι θέλουμε να συνδέσουμε δύο τερματικά στο σύστημα: ένα Wyse-50 και ένα παλιό IBM PC 286 στο οποίο εκτελούμε την εφαρμογή Procomm με την οποία εξομοιώνεται ένα τερματικό τύπου VT-100. Συνδέουμε το Wyse στη δεύτερη σειριακή θύρα και το 286 στην έκτη σειριακή θύρα (η οποία βρίσκεται σε μια κάρτα πολλαπλών θυρών). Οι αντίστοιχες καταχωρίσεις στο αρχείο /etc/ttys θα μοιάζουν με τις παρακάτω:

```
ttyu1  "/usr/libexec/getty std.38400"  wy50  on  insecure
ttyu5   "/usr/libexec/getty std.19200"  vt100  on  insecure
```

- Το πρώτο πεδίο, είναι συνήθως το όνομα του ειδικού αρχείου τερματικού όπως φαίνεται στον κατάλογο /dev.
- Το δεύτερο πεδίο, είναι η εντολή που θα εκτελεστεί για αυτή τη γραμμή, η οποία είναι συνήθως η getty(8). Η `getty` αρχικοποιεί και ανοίγει τη γραμμή, ρυθμίζει την ταχύτητα, εμφανίζει την προτροπή για εισαγωγή ονόματος χρήστη, και εκτελεί το πρόγραμμα login(1).Το πρόγραμμα `getty` δέχεται μια (προαιρετική) παράμετρο στη γραμμή εντολής του, τον τύπο του *getty*. Ο τύπος του *getty* καθορίζει τα χαρακτηριστικά της γραμμής του τερματικού, όπως π.χ. το ρυθμό μετάδοσης σε bps και την ισοτιμία (parity). Το πρόγραμμα `getty` διαβάζει αυτά τα χαρακτηριστικά από το αρχείο /etc/gettytab.Το αρχείο /etc/gettytab περιέχει πολλές καταχωρίσεις για γραμμές τερματικών, τόσο παλιές όσο και καινούριες. Στις περισσότερες από αυτές τις περιπτώσεις, οι καταχωρίσεις που ξεκινούν με το κείμενο `std`, θα λειτουργήσουν για απευθείας συνδεδεμένα τερματικά. Αυτές οι καταχωρίσεις αγνοούν την ισοτιμία. Υπάρχει μια καταχώριση `std` για κάθε ρυθμό μετάδοσης, από 110 ως 115200. Φυσικά, μπορείτε να προσθέσετε τις δικές σας καταχωρίσεις σε αυτό το αρχείο. Η σελίδα manual του gettytab(5) περιέχει περισσότερες πληροφορίες.Όταν ρυθμίζετε τον τύπο της *getty* στο αρχείο /etc/ttys, βεβαιωθείτε ότι ταιριάζουν οι αντίστοιχες ρυθμίσεις επικοινωνιών στο τερματικό σας.Στο παράδειγμα μας, το Wyse-50 δεν χρησιμοποιεί ισοτιμία και συνδέεται στα 38400 bps. Το 286 PC δεν χρησιμοποιεί ισοτιμία, και συνδέεται στα 19200 bps.
- Το τρίτο πεδίο είναι ο τύπος του τερματικού που συνδέεται συνήθως σε αυτή τη γραμμή tty. Για θύρες επιλογικών συνδέσεων (dial-up), η τιμή αυτού του πεδίου συχνά θα είναι `unknown` ή `dialup`, καθώς οι χρήστες θα μπορούν να πραγματοποιήσουν σύνδεση με οποιοδήποτε λογισμικό ή τερματικό. Για άμεσα συνδεμένα τερματικά, ο τύπος τερματικού δεν αλλάζει, έτσι μπορείτε να βάλετε ένα πραγματικό τύπο τερματικού σε αυτό το πεδίο, τον οποίο θα βρείτε στη βάση δεδομένων του termcap(5).Για παράδειγμα, το Wyse-50 χρησιμοποιεί τον πραγματικό τύπο τερματικού του, ενώ το 286 PC που εκτελεί το Procomm, έχει ρυθμιστεί να εξομοιώνει τερματικό τύπου VT-100.
- Το τέταρτο πεδίο καθορίζει αν η θύρα θα είναι ενεργή. Τοποθετώντας εδώ τη λέξη `on`, η `init`

θα ξεκινήσει το πρόγραμμα που αναφέρεται στο δεύτερο πεδίο, την `getty`. Αν βάλετε `off` σε αυτό το πεδίο, δεν θα εκτελεστεί η `getty`, και έτσι δεν θα μπορεί να γίνει είσοδος στο σύστημα από τη συγκεκριμένη θύρα.

- Το τελευταίο πεδίο χρησιμοποιείται για να καθορίσει αν η θύρα είναι ασφαλής. Αν χαρακτηρίσετε μια θύρα ως ασφαλή, σημαίνει ότι την εμπιστεύεστε αρκετά ώστε να επιτρέπετε την είσοδο του `root` μέσω αυτής (ή οποιουδήποτε λογαριασμού με ID 0). Δεν επιτρέπεται η είσοδος του `root` σε μια θύρα που έχει χαρακτηριστεί μη-ασφαλής. Σε μη-ασφαλείς θύρες, οι χρήστες πρέπει να εισέρχονται χρησιμοποιώντας ένα συνηθισμένο λογαριασμό χρήστη, και να χρησιμοποιούν την εντολή su(1) ή άλλο αντίστοιχο μηχανισμό για να αποκτήσουν προνόμια υπερχρήστη.Σας συνιστούμε ανεπιφύλακτα να χρησιμοποιήσετε τη ρύθμιση "insecure", ακόμα και για τερματικά που βρίσκονται σε κλειδωμένα δωμάτια. Είναι αρκετά εύκολο να εισέλθετε ως κανονικός χρήστης και να χρησιμοποιήσετε την εντολή `su` αν χρειάζεστε προνόμια υπερχρήστη.

48.2.2. Εξαναγκάστε την `init` να Ξαναδιαβάσει το /etc/ttys

Έχοντας κάνει τις απαραίτητες αλλαγές στο αρχείο /etc/ttys, θα πρέπει να στείλετε σήμα SIGHUP (hangup) στην διεργασία `init` για να την αναγκάσετε να διαβάσει ξανά το αρχείο ρυθμίσεων της. Για παράδειγμα:

```
# kill -HUP 1
```

Η `init` είναι πάντοτε η πρώτη διεργασία που εκτελείται σε ένα σύστημα, και έτσι θα έχει πάντοτε τον αριθμό διεργασίας (PID) 1.

Αν όλες οι ρυθμίσεις είναι σωστές, τα καλώδια είναι στη θέση τους, και τα τερματικά είναι ενεργά, θα εκτελεστεί η `getty` σε κάθε τερματικό, και στο σημείο αυτό θα δείτε την προτροπή εισόδου (login) στις οθόνες των τερματικών σας.

48.3. Αντιμετώπιση Προβλημάτων Σύνδεσης

Ακόμα και αν δώσετε μεγάλη προσοχή στις λεπτομέρειες, πάντα μπορεί να πάει κάτι στραβά όταν ρυθμίζετε ένα τερματικό. Εδώ θα βρείτε μια λίστα από συμπτώματα και συνιστώμενες διορθώσεις.

48.3.1. Δεν Εμφανίζεται Προτροπή Εισόδου (login)

Βεβαιωθείτε ότι το τερματικό είναι συνδεμένο στο ηλεκτρικό δίκτυο και ενεργοποιημένο. Αν είναι προσωπικός υπολογιστής που ενεργεί ως τερματικό, βεβαιωθείτε ότι εκτελεί λογισμικό εξομοίωσης τερματικού στην σωστή σειριακή θύρα.

Βεβαιωθείτε ότι το καλώδιο είναι καλά συνδεμένο τόσο στο τερματικό, όσο και στον υπολογιστή που εκτελεί FreeBSD. Βεβαιωθείτε ότι είναι το σωστό είδος καλωδίου.

Βεβαιωθείτε ότι το τερματικό και το FreeBSD συμφωνούν όσο αφορά τις ρυθμίσεις της ταχύτητας μετάδοσης και ισοτιμίας. Ελέγξτε τη φωτεινότητα και την αντίθεση της οθόνης του τερματικού, και αυξήστε τις αν χρειάζεται. Αν πρόκειται για τερματικό με εκτυπωτή (χωρίς οθόνη), βεβαιωθείτε ότι

διαθέτει επάρκεια χαρτιού και μελανιού.

Βεβαιωθείτε ότι εκτελείται η διαδικασία `getty` που εξυπηρετεί το τερματικό. Για να δείτε μια λίστα με τις ενεργές διαδικασίες `getty`, χρησιμοποιήστε την εντολή `ps`:

```
# ps -axww|grep getty
```

Θα πρέπει να δείτε μια καταχώριση για το τερματικό σας. Για παράδειγμα, η ακόλουθη οθόνη δείχνει ότι η διεργασία `getty` εκτελείτε στη δεύτερη σειριακή θύρα ttyu1 και χρησιμοποιεί την καταχώριση `std.38400` στο αρχείο /etc/gettytab:

```
22189  d1  Is+    0:00.03 /usr/libexec/getty std.38400 ttyu1
```

Αν δεν εκτελείται καμιά διεργασία `getty`, βεβαιωθείτε ότι έχετε ενεργοποιήσει τη θύρα στο /etc/ttys. Επίσης θυμηθείτε να εκτελέσετε την εντολή `kill -HUP 1` μετά την τροποποίηση του αρχείου ttys.

Αν εκτελείται η διεργασία `getty` αλλά το τερματικό εξακολουθεί να μη δείχνει προτροπή εισόδου, ή αν δείχνει προτροπή αλλά δεν σας επιτρέπει να γράψετε, ίσως το τερματικό σας ή το καλώδιο να μην επιτρέπουν συνεννόηση μέσω υλικού (hardware handshake). Δοκιμάστε να αλλάξετε την καταχώριση στο αρχείο /etc/ttys από `std.38400` σε `3wire.38400` (θυμηθείτε να εκτελέσετε την εντολή `kill -HUP 1` μετά την τροποποίηση του /etc/ttys). Η καταχώριση `3wire` είναι αντίστοιχη με την `std`, αλλά αγνοεί το hardware handshaking. Μπορεί επίσης να χρειαστεί να μειώσετε το ρυθμό σηματοδοσίας (baud) και να ενεργοποιήσετε τον έλεγχο ροής μέσω λογισμικού όταν χρησιμοποιείτε το `3wire`, προκειμένου να αποφύγετε υπερχείλιση της προσωρινής μνήμης (buffer overflow).

48.3.2. Αν Βλέπετε Σκουπίδια Αντί για Προτροπή Εισόδου

Βεβαιωθείτε ότι το τερματικό και το FreeBSD συμφωνούν στο ρυθμό bps και στις ρυθμίσεις ισοτιμίας. Ελέγξτε τις διεργασίες `getty` για να βεβαιωθείτε ότι εκτελείτε το σωστό τύπο *getty*. Αν αυτό δεν συμβαίνει, επεξεργαστείτε το αρχείο /etc/ttys και εκτελέστε την εντολή `kill -HUP 1`.

48.3.3. Οι Χαρακτήρες Εμφανίζονται Διπλοί, το Password Εμφανίζεται κατά την Πληκτρολόγηση

Αλλάξτε τη ρύθμιση του τερματικού (ή του προγράμματος εξομοίωσης τερματικού) από "half duplex" ή "local echo" σε "full duplex".

Chapter 49. Υπηρεσία Εισόδου μέσω Επιλογικής Σύνδεσης (dial-in)

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών των σειριακών θυρών μετονομάστηκαν από /dev/cuadN σε /dev/cuauN και από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την παρακάτω τεκμηρίωση σύμφωνα με τις παραπάνω αλλαγές.

Η ρύθμιση του FreeBSD συστήματος σας για είσοδο μέσω επιλογικής σύνδεσης, είναι αρκετά όμοια με τη σύνδεση τερματικών, εκτός από το γεγονός ότι χρησιμοποιούνται modems αντί για τερματικά.

49.1. Εξωτερικά και Εσωτερικά Modems

Τα εξωτερικά modems είναι μάλλον πιο βολικά για επιλογικές κλήσεις, καθώς οι περισσότερες ρυθμίσεις τους μπορούν να αποθηκευθούν μόνιμα στη μή-πτητική μνήμη RAM που διαθέτουν. Τα εξωτερικά modems διαθέτουν συνήθως φωτεινές ενδείξεις που δείχνουν την κατάσταση σημαντικών σημάτων του RS-232. Ίσως τα φωτάκια που αναβοσβήνουν να εντυπωσιάζουν τους επισκέπτες, αλλά είναι επίσης χρήσιμα για να φαίνεται πότε το modem λειτουργεί σωστά.

Τα εσωτερικά modems συνήθως δεν διαθέτουν αυτή τη μνήμη RAM, και έτσι οι ρυθμίσεις τους περιορίζονται μόνο στην αλλαγή θέσης σε κάποιους διακόπτες ρυθμίσεων (DIP switches). Αν το εσωτερικό σας modem διαθέτει φωτεινές ενδείξεις, μάλλον θα είναι δύσκολο να τις δείτε όταν το κάλυμμα του συστήματος σας είναι στη θέση του.

49.1.1. Modems και Καλώδια

Αν χρησιμοποιείτε εξωτερικό modem, θα χρειαστείτε φυσικά το σωστό καλώδιο. Συνήθως επαρκεί το τυποποιημένο καλώδιο RS-232C, εφόσον διαθέτει συνδέσεις για όλα τα συνηθισμένα σήματα:

Πίνακας 7. Ονομασίες Σημάτων

Ακρωνύμια	Ονόματα
RD	Λήψη Δεδομένων (Received Data)
TD	Αποστολή Δεδομένων (Transmitted Data)
DTR	Τερματικό Δεδομένων σε Ετοιμότητα (Data Terminal Ready)
DSR	Σύνολο Δεδομένων σε Ετοιμότητα (Data Set Ready)
DCD	Ανίχνευση Φέροντος Σήματος (Data Carrier Detect). Ανίχνευση σύνδεσης της γραμμής RS-232C
SG	Γείωση Σήματος (Signal Ground)
RTS	Αίτηση Αποστολής (Request to Send)

Ακρωνύμια	Ονόματα
CTS	Ετοιμότητα για Αποστολή (Clear to Send)

Το FreeBSD χρειάζεται τα σήματα RTS και CTS για έλεγχο ροής σε ταχύτητες πάνω από 2400 bps, το σήμα CD για να ανιχνεύει πότε έχει απαντηθεί μια κλήση ή πότε η γραμμή έχει κλείσει, και το σήμα DTR για να επαναφέρει το modem στην αρχική του κατάσταση μετά τη λήξη μιας σύνδεσης. Μερικά καλώδια δεν διαθέτουν όλα τα απαραίτητα σήματα, έτσι αν έχετε προβλήματα με τον τερματισμό της συνεδρίας εισόδου με το κλείσιμο της γραμμής, πιθανόν να ευθύνεται το καλώδιο που χρησιμοποιείτε.

Όπως και άλλα λειτουργικά συστήματα τύπου UNIX®, το FreeBSD χρησιμοποιεί τα σήματα του υλικού για να αντιληφθεί πότε έχει απαντηθεί μια κλήση, καθώς και για τον τερματισμό της και την επαναφορά του modem στην αρχική του κατάσταση μετά το τέλος της. Το FreeBSD αποφεύγει να στέλνει εντολές στο modem ή να παρακολουθεί αναφορές κατάστασης από αυτό. Αν είστε εξοικειωμένος με συνδέσεις modems σε BBS (Bulletin Board Systems) που βασίζονται σε PC, αυτό μπορεί να σας φανεί άβολο.

49.2. Κυκλώματα Σειριακής Διασύνδεσης

Το FreeBSD υποστηρίζει τα κυκλώματα επικοινωνιών που βασίζονται στα NS8250, NS16450, NS16550, και NS16550A και EIA RS-232C (CCITT V.24). Οι συσκευές 8250 και 16450 έχουν ενδιάμεση μνήμη (buffer) μεγέθους ενός χαρακτήρα. Η συσκευή 16550 διαθέτει ενδιάμεση μνήμη 16 χαρακτήρων, η οποία επιτρέπει την καλύτερη απόδοση της. (Λόγω προβλημάτων στη σχεδίαση του 16550, δεν είναι δυνατή η χρήση αυτής της μνήμης, αν είναι δυνατόν χρησιμοποιήστε τα 16550A). Καθώς οι συσκευές που διαθέτουν ενδιάμεση μνήμη ενός χαρακτήρα απαιτούν περισσότερη εργασία από το λειτουργικό σύστημα σε σχέση με αυτές που διαθέτουν 16 χαρακτήρες, συνίστανται ιδιαίτερα οι συσκευές που βασίζονται στο 16550A. Αν το σύστημα σας έχει πολλές ενεργές σειριακές πόρτες, ή πρόκειται να λειτουργήσει κάτω από βαρύ φόρτο, οι κάρτες που βασίζονται στο 16550A είναι καλύτερες, καθώς παρέχουν επικοινωνία με μικρότερο ρυθμό σφαλμάτων.

49.3. Γρήγορη Επισκόπηση

Όπως και με τα τερματικά, η `init` εκτελεί μια διεργασία `getty` για κάθε σειριακή θύρα που έχει ρυθμιστεί για εισερχόμενες επιλογικές συνδέσεις. Για παράδειγμα, αν έχετε συνδέσει ένα modem στη θύρα /etc/ttyu0, η εντολή `ps ax` θα δείξει κάτι σαν το παρακάτω:

```
4850 ??  I      0:00.09 /usr/libexec/getty V19200 ttyu0
```

Όταν κάποιος χρήστης καλέσει στη γραμμή αυτή και το modem συνδεθεί, ενεργοποιείται από το modem η γραμμή CD. Ο πυρήνας παρατηρεί ότι έχει ανιχνευθεί φέρον σήμα, και ολοκληρώνει τη διαδικασία ανοίγματος της θύρας από το modem. Το `getty` στέλνει μια προτροπή `login:` στην από πριν καθορισμένη αρχική ταχύτητα της θύρας. Το `getty` παρακολουθεί για να δει αν λαμβάνονται έγκυροι χαρακτήρες, και στην τυπική ρύθμιση, αν ανακαλύψει ότι λαμβάνει σκουπίδια (πιθανώς λόγω διαφοράς στην ταχύτητα σύνδεσης του modem σε σχέση με την ταχύτητα του `getty`), προσπαθεί να ρυθμίσει την ταχύτητα της γραμμής μέχρι να λάβει φυσιολογικούς χαρακτήρες.

Αφού ο χρήστης εισάγει τον κωδικό του, το getty εκτελεί το /usr/bin/login, το οποίο και ολοκληρώνει τη διαδικασία εισόδου, ζητώντας από τον χρήστη τον κωδικό του, και ξεκινώντας έπειτα το κέλυφος του.

49.4. Αρχεία Ρυθμίσεων

Υπάρχουν τρία αρχεία ρυθμίσεων συστήματος στον κατάλογο /etc, τα οποία πιθανώς θα χρειαστεί να επεξεργαστείτε για να επιτρέψετε την είσοδο μέσω επιλογικής σύνδεσης στο FreeBSD σύστημα σας. Το πρώτο αρχείο είναι το /etc/gettytab, το οποίο περιέχει πληροφορίες ρύθμισης για τον δαίμονα /usr/libexec/getty Το δεύτερο αρχείο είναι το /etc/ttys το οποίο περιέχει πληροφορίες που γνωστοποιούν στην /sbin/init σε ποιες συσκευές tty θα πρέπει να εκτελούνται διεργασίες getty. Τέλος, μπορείτε να βάλετε εντολές αρχικοποίησης της θύρας στο script /etc/rc.d/serial.

Υπάρχουν δύο "σχολές" όσο αφορά τη χρήση modems για είσοδο σε ένα σύστημα UNIX®. Η πρώτη, προτιμά να ρυθμίζει τα modems και τα συστήματα με τέτοιο τρόπο, ώστε άσχετα με τι ταχύτητα συνδέεται ο απομακρυσμένος χρήστης, η τοπική σύνδεση υπολογιστή - modem μέσω του RS-232C να έχει πάντα την ίδια κλειδωμένη ταχύτητα. Το όφελος μιας τέτοιας ρύθμισης είναι ότι ο απομακρυσμένος χρήστης βλέπει πάντα άμεσα την προτροπή εισόδου. Το μειονέκτημα, είναι ότι το σύστημα δεν γνωρίζει την πραγματική ταχύτητα σύνδεσης του χρήστη, και έτσι προγράμματα πλήρους οθόνης όπως το Emacs, δεν γνωρίζουν πως να ρυθμίσουν την ταχύτητα ανανέωσης της οθόνης τους ώστε να αντιμετωπίσουν καλύτερα τις αργές συνδέσεις.

Η άλλη σχολή ρυθμίζει τη διεπαφή RS-232 του modem να αλλάζει ταχύτητα, ώστε να ακολουθεί την ταχύτητα σύνδεσης του απομακρυσμένου χρήστη. Για παράδειγμα, συνδέσεις τύπου V.32bis (14.4 Kbps) στο modem, μπορεί να το κάνουν να μεταβάλλει την ταχύτητα σύνδεσης στο RS-232 σε 19.2 Kbps, ενώ συνδέσεις ταχύτητας 2400 bps θα μεταβάλλουν αντίστοιχα την ταχύτητα της διεπαφής σε 2400 bps. Επειδή η getty δεν αναγνωρίζει με κάποιο τρόπο την ταχύτητα σύνδεσης που αναφέρει το modem, δίνει την πρώτη προτροπή login: στην αρχικά ρυθμισμένη ταχύτητα, και εξετάζει τους χαρακτήρες που λαμβάνει ως απάντηση. Αν ο χρήστης δει σκουπίδια, θεωρείται ότι γνωρίζει ότι πρέπει να πιέσει το Enter μέχρι να πάρει μια προτροπή που μπορεί να αναγνωρίσει. Αν οι ρυθμοί δεδομένων δεν ταιριάζουν, η getty βλέπει οτιδήποτε γράφει ο χρήστης ως "σκουπίδια", και έτσι δοκιμάζει την επόμενη ταχύτητα και στέλνει ξανά την προτροπή login:. Η διαδικασία μπορεί να επαναληφθεί όσες φορές χρειάζεται, αλλά συνήθως χρειάζονται μόνο μια-δυο προσπάθειες μέχρι ο χρήστης να λάβει κανονική προτροπή. Προφανώς αυτή η ακολουθία εισόδου δεν είναι τόσο καθαρή όπως η προηγούμενη μέθοδος "κλειδωμένης ταχύτητας", αλλά κάποιος χρήστης που βρίσκεται σε γραμμή χαμηλής ταχύτητας, μάλλον θα λάβει καλύτερη απόκριση σε εφαρμογές πλήρους οθόνης.

Σε αυτή την ενότητα θα προσπαθήσουμε να σας δώσουμε πληροφορίες και για τους δύο τύπους ρυθμίσεων, αλλά θεωρούμε καλύτερο το είδος σύνδεσης όπου η ταχύτητα υπολογιστή - modem ακολουθεί την ταχύτητα της σύνδεσης.

49.4.1. /etc/gettytab

Το /etc/gettytab είναι ένα αρχείο τύπου termcap(5) με πληροφορίες ρύθμισης για την getty(8). Παρακαλούμε δείτε τη σελίδα manual gettytab(5) για πιο πλήρεις πληροφορίες σχετικά με τη μορφή του αρχείου και την λίστα με τις δυνατότητες του.

49.4.1.1. Ρύθμιση για Κλειδωμένη Ταχύτητα

Αν πρόκειται να κλειδώσετε την επικοινωνία του modem σας σε μια συγκεκριμένη ταχύτητα, κατά πάσα πιθανότητα δεν θα χρειαστεί να κάνετε αλλαγές στο /etc/gettytab.

49.4.1.2. Ρύθμιση για Μεταβλητή Ταχύτητα

θα χρειαστεί να προσθέσετε μια καταχώριση στο /etc/gettytab για να δώσετε πληροφορίες στην `getty` σχετικά με τις ταχύτητες που επιθυμείτε να χρησιμοποιήσετε στο modem σας. Αν έχετε ένα modem 2400 bps, μπορείτε πιθανόν να χρησιμοποιήσετε την καταχώριση `D2400`.

```
#
# Fast dialup terminals, 2400/1200/300 rotary (can start either way)
#
D2400|d2400|Fast-Dial-2400:\
        :nx=D1200:tc=2400-baud:
3|D1200|Fast-Dial-1200:\
        :nx=D300:tc=1200-baud:
5|D300|Fast-Dial-300:\
        :nx=D2400:tc=300-baud:
```

Αν έχετε modem υψηλότερης ταχύτητας, πιθανόν να χρειαστεί να προσθέσετε μια καταχώριση στο /etc/gettytab. Παρακάτω φαίνεται μια καταχώριση που μπορεί να χρησιμοποιηθεί για modem 14.4 Kbps με μέγιστη ταχύτητα σειριακής θύρας 19.2 Kbps:

```
#
# Additions for a V.32bis Modem
#
um|V300|High Speed Modem at 300,8-bit:\
        :nx=V19200:tc=std.300:
un|V1200|High Speed Modem at 1200,8-bit:\
        :nx=V300:tc=std.1200:
uo|V2400|High Speed Modem at 2400,8-bit:\
        :nx=V1200:tc=std.2400:
up|V9600|High Speed Modem at 9600,8-bit:\
        :nx=V2400:tc=std.9600:
uq|V19200|High Speed Modem at 19200,8-bit:\
        :nx=V9600:tc=std.19200:
```

Αυτό θα έχει ως αποτέλεσμα συνδέσεις 8bit χωρίς ισοτιμία.

Το παραπάνω παράδειγμα, ξεκινά το ρυθμό επικοινωνίας στα 19.2 Kbps (για μια σύνδεση V.32bis), και έπειτα δοκιμάζει κυκλικά στα 9600 bps (για V.32), 2400 bps, 1200 bps, 300 bps, και πίσω στα 19.2 Kbps. Αυτή η κυκλική εναλλαγή ρυθμού επιτυγχάνεται με την ικανότητα `nx=` ("next table"). Κάθε μια από τις γραμμές χρησιμοποιεί μια καταχώριση `tc=` ("table continuation") για να βρει τις υπόλοιπες "τυποποιημένες" ρυθμίσεις για κάποιο συγκεκριμένο ρυθμό μετάδοσης δεδομένων.

Αν έχετε modem 28.8 Kbps ή/και θέλετε να επωφεληθείτε από την συμπίεση ενός modem 14.4 Kbps,

θα πρέπει να χρησιμοποιήσετε ρυθμό επικοινωνίας μεγαλύτερο από 19.2 Kbps. Παρακάτω φαίνεται ένα παράδειγμα μια καταχώρισης στο gettytab που ξεκινάει από τα 57.6 Kbps:

```
#
# Additions for a V.32bis or V.34 Modem
# Starting at 57.6 Kbps
#
vm|VH300|Very High Speed Modem at 300,8-bit:\
        :nx=VH57600:tc=std.300:
vn|VH1200|Very High Speed Modem at 1200,8-bit:\
        :nx=VH300:tc=std.1200:
vo|VH2400|Very High Speed Modem at 2400,8-bit:\
        :nx=VH1200:tc=std.2400:
vp|VH9600|Very High Speed Modem at 9600,8-bit:\
        :nx=VH2400:tc=std.9600:
vq|VH57600|Very High Speed Modem at 57600,8-bit:\
        :nx=VH9600:tc=std.57600:
```

Αν έχετε αργό επεξεργαστή ή μεγάλο φορτίο, και το σύστημα σας δεν διαθέτει σειριακές θύρες που να βασίζονται στο 16550A, ίσως λάβετε λάθη `sio` "silo" στα 57.6 Kbps.

49.4.2. /etc/ttys

Έχουμε ήδη καλύψει τη ρύθμιση του αρχείου /etc/ttys στο Προσθήκη Καταχωρίσεων για τα Τερματικά στο /etc/ttys. Η ρύθμιση για modems είναι παρόμοια, αλλά πρέπει να δώσουμε διαφορετικό όρισμα στην `getty` και να καθορίσουμε διαφορετικό τύπο τερματικού. Η γενική μορφή τόσο για κλειδωμένη όσο και για μεταβλητή ταχύτητα είναι η παρακάτω:

```
ttyu0   "/usr/libexec/getty xxx"   dialup on
```

Το πρώτο πεδίο στην παραπάνω γραμμή είναι το ειδικό αρχείο συσκευής για αυτή την καταχώριση - το ttyu0 αντιστοιχεί στο αρχείο /dev/ttyu0 το οποίο και θα παρακολουθεί η `getty`. Το δεύτερο πεδίο, `"/usr/libexec/getty xxx"` (το *xxx* θα έχει την αρχική τιμή ικανότητας του gettytab), είναι η διεργασία που θα εκτελέσει η `init` στη συσκευή. Το τρίτο πεδίο, `dialup`, είναι ο προεπιλεγμένος τύπος τερματικού. Η τέταρτη παράμετρος, `on`, δείχνει στην `init` ότι η γραμμή είναι σε λειτουργική κατάσταση. Μπορεί να υπάρχει και μια πέμπτη παράμετρος, η `secure`, αλλά θα πρέπει να χρησιμοποιείται μόνο για τερματικά στα οποία η φυσική πρόσβαση είναι ασφαλής (όπως είναι η κονσόλα του συστήματος).

Ο προεπιλεγμένος τύπος τερματικού (`dialup` στο παραπάνω παράδειγμα) μπορεί να αλλάξει ανάλογα με τις προτιμήσεις σας. Το `dialup` είναι ο παραδοσιακός τύπος τερματικού για επιλογικές γραμμές. Οι χρήστες μπορούν έτσι να προσαρμόζουν τα scripts σύνδεσης τους ώστε να αναγνωρίζουν το `dialup` και να ρυθμίζουν αυτόματα τον τύπο τερματικού. Ωστόσο, είναι μάλλον ευκολότερο να καθορίσετε το `vt102` ως τον προεπιλεγμένο τύπο τερματικού, καθώς οι χρήστες χρησιμοποιούν συνήθως εξομοίωση VT102 στα απομακρυσμένα τους συστήματα.

Αφού κάνετε τις αλλαγές στο /etc/ttys, μπορείτε να στείλετε στη διεργασία `init` ένα σήμα HUP για να

ξαναδιαβάσει το αρχείο. Μπορείτε να χρησιμοποιήσετε την παρακάτω εντολή για αυτό το σκοπό:

```
# kill -HUP 1
```

Αν αυτή είναι η πρώτη φορά που ρυθμίζετε το σύστημα σας, ίσως θέλετε να περιμένετε μέχρι να ολοκληρώσετε πλήρως τη σύνδεση και ρύθμιση του modem σας πριν στείλετε σήμα στην `init`.

49.4.2.1. Ρύθμιση για Κλειδωμένη Ταχύτητα

Για λειτουργία σε κλειδωμένη ταχύτητα, θα πρέπει η καταχώριση σας στο ttys να παρέχει στην `getty` μια καταχώριση σταθερής ταχύτητας. Για ένα modem με ταχύτητα θύρας κλειδωμένη στα 19.2 Kbps, η καταχώριση ttys θα μοιάζει με την παρακάτω:

```
ttyu0   "/usr/libexec/getty std.19200"   dialup on
```

Αν το modem σας είναι κλειδωμένο σε διαφορετικό ρυθμό δεδομένων, αντικαταστήστε με την κατάλληλη τιμή το `std.19200` στην καταχώριση `std.speed`. Βεβαιωθείτε ότι χρησιμοποιείτε ένα έγκυρο τύπο, όπως ορίζεται στο /etc/gettytab.

49.4.2.2. Ρύθμιση για Μεταβλητή Ταχύτητα

Σε μια τέτοια ρύθμιση, η καταχώριση σας για το ttys θα πρέπει να αναφέρεται στην αρχική "auto-baud" (sic) καταχώριση του /etc/gettytab. Για παράδειγμα, αν προσθέσατε την παραπάνω συνιστώμενη καταχώριση για modem με μεταβλητή ταχύτητας σειριακής, και με αρχική ταχύτητα τα 19.2 Kbps (την καταχώριση gettytab που περιέχει ως σημείο εκκίνησης το `V19200`), η καταχώριση σας στο ttys θα μοιάζει με την παρακάτω:

```
ttyu0   "/usr/libexec/getty V19200"   dialup on
```

49.4.3. /etc/rc.d/serial

Τα modems υψηλής ταχύτητας, όπως τα V.32, V.32bis και V.34, απαιτούν έλεγχο ροής μέσω υλικού (`RTS/CTS`). Μπορείτε να προσθέσετε εντολές `stty` στο /etc/rc.d/serial για να θέσετε στον πυρήνα του FreeBSD την κατάλληλη παράμετρο έλεγχου ροής μέσω υλικού των θυρών modem.

Για παράδειγμα, για να θέσετε την επιλογή `termios` στην τιμή `crtscts` στις συσκευές αρχικοποίησης της δεύτερης σειριακής θύρας (COM2) για επιλογικές κλήσεις εισόδου και εξόδου, θα πρέπει να προσθέσετε τις παρακάτω γραμμές στο αρχείο /etc/rc.d/serial:

```
# Serial port initial configuration
stty -f /dev/ttyu1.init crtscts
stty -f /dev/cuau1.init crtscts
```

49.5. Ρυθμίσεις Μνήμης

Αν έχετε ένα modem στο οποίο μπορείτε να αποθηκεύσετε τις παραμέτρους μόνιμα στην μη-πτητική RAM που διαθέτει, θα πρέπει να χρησιμοποιήσετε ένα πρόγραμμα τερματικού (όπως το Telix μέσω του MS-DOS® ή του `tip` στο FreeBSD) για να ρυθμίσετε τις παραμέτρους. Συνδεθείτε στο modem χρησιμοποιώντας την ίδια αρχική ταχύτητα επικοινωνίας με αυτή που έχετε δηλώσει ως αρχική ταχύτητα στην `getty`, και ρυθμίστε τις παραμέτρους στη μνήμη του ώστε να ταιριάζουν με τις παρακάτω απαιτήσεις:

- Το σήμα CD θα είναι ενεργό όταν το modem είναι συνδεμένο
- Το σήμα DTR θα είναι ενεργό κατά τη λειτουργία. Απενεργοποίηση του DTR κλείνει τη γραμμή και επαναφέρει το modem στην αρχική του κατάσταση.
- Το CTS θα χρησιμοποιείται για έλεγχο ροής μεταδιδόμενων δεδομένων
- Ο έλεγχος ροής XON/XOFF θα είναι ανενεργός
- Το RTS θα χρησιμοποιείται για έλεγχο ροής ληφθέντων δεδομένων
- Ήσυχη λειτουργία (Quiet mode, χωρίς αποστολή κωδικών αποτελεσμάτων)
- Δεν θα γίνεται echo των εντολών

Θα πρέπει να διαβάσετε την τεκμηρίωση του modem σας για να βρείτε τις εντολές που πρέπει να αποστείλετε. Ίσως επίσης χρειαστεί να αλλάξετε τη θέση κάποιων ρυθμιστικών διακοπτών (dip switches).

Για παράδειγμα, για να ρυθμίσετε τις παραπάνω παραμέτρους σε ένα εξωτερικό modem U.S. Robotics® Sportster® 14,400, θα έπρεπε να στείλετε τις παρακάτω εντολές στο modem:

```
ATZ
AT&C1&D2&H1&I0&R2&W
```

Μπορείτε με την ευκαιρία να ρυθμίσετε και άλλους παραμέτρους του modem, όπως για το αν θα χρησιμοποιείται το πρωτόκολλο V.42bis ή συμπίεση MNP5.

Το εξωτερικό modem U.S. Robotics® Sportster® 14,400 διαθέτει επίσης και κάποιους ρυθμιστικούς διακόπτες που πρέπει να ρυθμιστούν. Για άλλα modem, ίσως μπορείτε να χρησιμοποιήσετε αυτές τις ρυθμίσεις ως αναφορά:

- Διακόπτης 1: Άνω Θέση - Κανονική λειτουργία DTR
- Διακόπτης 2: N/A (Κωδικός Αποτελέσματος ως Κείμενο/Κωδικός Αποτελέσματος ως Αριθμός)
- Διακόπτης 3: Άνω θέση - Χωρίς Κωδικό Αποτελέσματος
- Διακόπτης 4: Κάτω θέση - Χωρίς echo και offline εντολές
- Διακόπτης 5: Άνω θέση - Αυτόματη Απάντηση
- Διακόπτης 6: Άνω θέση - Φυσιολογική Ανίχνευση Φέροντος Σήματος
- Διακόπτης 7: Άνω θέση - Φόρτωση Προεπιλογών από NVRAM (μη-πτητική μνήμη)
- Διακόπτης 8: N/A (Έξυπνος/Κουτός Τρόπος Λειτουργίας)

Θα πρέπει να απενεργοποιήσετε ή να απομονώσετε τους κωδικούς αποτελεσμάτων στο modem, για να αποφύγετε προβλήματα που μπορούν να δημιουργηθούν αν η `getty` από λάθος στείλει προτροπή `login:` στο modem ενώ αυτό βρίσκεται σε κατάσταση εντολών. Στην περίπτωση αυτή, το modem μπορεί να αναπαράγει ξανά την εντολή (echo) ή να στείλει κάποιο κωδικό αποτελέσματος. Αυτό μπορεί να έχει ως αποτέλεσμα μια μακρόχρονη και χαζή συνομιλία μεταξύ του modem και της `getty`.

49.5.1. Ρυθμίσεις για Κλειδωμένη Ταχύτητα

Για λειτουργία σε κλειδωμένη ταχύτητα, θα χρειαστεί να ρυθμίσετε το modem να διατηρεί σταθερή ταχύτητα υπολογιστή - modem, άσχετα με την ταχύτητα επικοινωνίας της επιλογικής σύνδεσης. Σε ένα εξωτερικό modem U.S. Robotics® Sportster® 14,400, οι εντολές αυτές θα κλειδώσουν την επικοινωνία υπολογιστή - modem στην ίδια ταχύτητα που έγινε η λήψη των εντολών:

```
ATZ
AT&B1&W
```

49.5.2. Ρυθμίσεις για Μεταβλητή Ταχύτητα

Για λειτουργία σε μεταβλητή ταχύτητα, θα χρειαστεί να ρυθμίσετε το modem σας να προσαρμόζει την ταχύτητα της σειριακής θύρας του ώστε να ταιριάζει με αυτή της εισερχόμενης κλήσης. Σε ένα εξωτερικό modem U.S. Robotics® Sportster® 14,400, οι εντολές αυτές θα κλειδώσουν την ταχύτητα μεταφοράς δεδομένων με διόρθωση λαθών του modem στην ταχύτητα που χρησιμοποιήθηκε για την αποστολή των εντολών, αλλά θα επιτρέψουν στην ταχύτητα της σειριακής θύρας να μεταβάλλεται για συνδέσεις που δεν έχουν διόρθωση λαθών:

```
ATZ
AT&B2&W
```

49.5.3. Έλεγχος των Ρυθμίσεων του Modem

Τα περισσότερα modem υψηλής ταχύτητας, παρέχουν εντολές με τις οποίες μπορείτε να παρακολουθήσετε τις τρέχουσες παραμέτρους λειτουργίας τους με σχετικά κατανοητό τρόπο. Στο εξωτερικό modem U.S. Robotics® Sportster® 14,400, η εντολή `ATI5` δείχνει τις ρυθμίσεις που είναι αποθηκευμένες στη μη-πτητική RAM του modem. Για να δείτε τις πραγματικές παραμέτρους λειτουργίας του modem (όπως αυτές επηρεάζονται από τις θέσεις των ρυθμιστικών διακοπτών του), χρησιμοποιήστε τις εντολές `ATZ` και μετά `ATI4`.

Αν διαθέτετε modem άλλης εταιρίας, ελέγξτε τις οδηγίες χρήσης του για να δείτε πως μπορείτε να ελέγξετε με σιγουριά τις παραμέτρους ρύθμισης του.

49.6. Αντιμετώπιση Προβλημάτων

Παρακάτω θα βρείτε μερικά βήματα που μπορείτε να ακολουθήσετε για να ελέγξετε τη λειτουργία του modem στο σύστημα σας.

49.6.1. Ελέγχοντας το Σύστημα σας

Συνδέστε το modem στο FreeBSD σύστημα σας, εκκινήστε το, και αν το modem σας διαθέτει φωτεινές ενδείξεις κατάστασης, παρακολουθήστε τις για να δείτε αν ενεργοποιείται η ένδειξη DTR όταν εμφανίζεται η προτροπή `login:` στην κονσόλα του συστήματος. Αν η ένδειξη αυτή είναι ενεργή, σημαίνει ότι το FreeBSD έχει ξεκινήσει μια διεργασία `getty` στην αντίστοιχη θύρα επικοινωνιών και αναμένει το modem να απαντήσει μια κλήση.

Αν δεν ενεργοποιείται η ένδειξη DTR, εισέλθετε στο σύστημα μέσω της κονσόλας, και δώστε την εντολή `ps ax` για να δείτε αν το FreeBSD προσπαθεί να εκτελέσει διεργασία `getty` στη σωστή θύρα. Ανάμεσα στις διεργασίες, θα δείτε γραμμές όπως τις παρακάτω:

```
114 ??  I      0:00.10 /usr/libexec/getty V19200 ttyu0
115 ??  I      0:00.10 /usr/libexec/getty V19200 ttyu1
```

Αν δείτε κάτι διαφορετικό, όπως το παρακάτω:

```
114 d0  I      0:00.10 /usr/libexec/getty V19200 ttyu0
```

και το modem δεν έχει απαντήσει ακόμα καμία κλήση, σημαίνει ότι η `getty` έχει ολοκληρώσει το άνοιγμα της σειριακής θύρας. Αυτό πιθανόν σημαίνει ότι υπάρχει πρόβλημα με την καλωδίωση, ή ότι το modem δεν είναι σωστά ρυθμισμένο, καθώς η `getty` δεν θα πρέπει να μπορεί να ανοίξει τη θύρα πριν ενεργοποιηθεί το σήμα CD (carrier detect, ανίχνευσης φέροντος) από το modem.

Αν δεν βλέπετε κάποιες διεργασίες `getty` να περιμένουν να ανοίξουν την επιθυμητή θύρα ttyuN, ελέγξτε ξανά τις καταχωρίσεις σας στο /etc/ttys για τυχόν λάθη. Ελέγξτε επίσης το αρχείο καταγραφής /var/log/messages για να δείτε αν υπάρχουν κάποια μηνύματα από την `init` ή την `getty` σχετικά με τα προβλήματα. Αν υπάρχουν μηνύματα, ελέγξτε ξανά τα αρχεία ρυθμίσεων /etc/ttys και /etc/gettytab, όπως και τα ειδικά αρχεία συσκευών /dev/ttyuN για πιθανά λάθη, ελλιπείς καταχωρίσεις, ή μη-ύπαρξη των ειδικών αρχείων συσκευών.

49.6.2. Προσπαθήστε να Εκτελέσετε Σύνδεση Εισόδου

Δοκιμάστε να εισέλθετε στο σύστημα σας μέσω απομακρυσμένης σύνδεσης. Βεβαιωθείτε ότι χρησιμοποιείτε 8 bits, 1 stop bit και επικοινωνία χωρίς ισοτιμία στο απομακρυσμένο σύστημα. Αν δε λάβετε άμεσα την προτροπή εισόδου, ή αν λαμβάνετε σκουπίδια, δοκιμάστε να πιέζετε `Enter` με ρυθμό περίπου μια φορά το δευτερόλεπτο. Αν ακόμα δεν λαμβάνετε την προτροπή `login:`, δοκιμάστε μετά από λίγο να στείλετε ένα `BREAK`. Αν κάνετε κλήση από ένα modem υψηλής ταχύτητας, δοκιμάστε ξανά, αφού κλειδώσετε την ταχύτητα επικοινωνίας υπολογιστή - modem από το οποίο καλείτε (μέσω π.χ. της `AT&B1` σε ένα U.S. Robotics® Sportster® modem).

Αν δεν μπορείτε ακόμα να λάβετε προτροπή `login:`, ελέγξτε ξανά και ξανά το αρχείο /etc/gettytab.

- Το όνομα της αρχικής ικανότητας που καθορίζεται στο αρχείο /etc/ttys για τη γραμμή πρέπει να ταιριάζει με το όνομα της ικανότητας στο /etc/gettytab
- Κάθε καταχώριση `nx=` ταιριάζει με το όνομα μιας αντίστοιχης ικανότητας στο gettytab

- Κάθε καταχώριση `tc=` ταιριάζει με το όνομα μιας αντίστοιχης ικανότητας στο gettytab

Αν κάνετε κλήση αλλά το modem στο FreeBSD σύστημα δεν απαντάει, βεβαιωθείτε ότι το modem είναι ρυθμισμένο να απαντάει την τηλεφωνική γραμμή όταν ενεργοποιείται το σήμα DTR. Αν το modem φαίνεται να είναι ρυθμισμένο σωστά, επαληθεύστε ότι η γραμμή DTR είναι ενεργή ελέγχοντας τις φωτεινές ενδείξεις του modem (αν υπάρχουν).

Αν έχετε ελέγξει τα πάντα πολλές φορές, και ακόμα δεν φαίνεται να βρίσκετε τη λύση, κάντε ένα διάλειμμα και προσπαθήστε ξανά αργότερα. Αν ακόμα δεν λειτουργεί, ίσως είναι καλή ιδέα να στείλετε ένα μήνυμα στην ηλεκτρονική λίστα γενικών ερωτήσεων του FreeBSD περιγράφοντας το πρόβλημα σας και το modem σας, και οι καλοί άνθρωποι που παρακολουθούν την λίστα θα προσπαθήσουν να σας βοηθήσουν.

Chapter 50. Υπηρεσία Επιλογικής Σύνδεσης

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών των σειριακών θυρών μετονομάστηκαν από /dev/cuadN σε /dev/cuauN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την παρακάτω τεκμηρίωση σύμφωνα με τις παραπάνω αλλαγές.

Παρακάτω θα βρείτε κάποιες συμβουλές για να μπορέσετε να συνδέσετε τον υπολογιστή σας μέσω modem σε κάποιο άλλο υπολογιστή. Με τον τρόπο αυτό, μπορείτε να δημιουργήσετε σύνδεση τερματικού προς ένα απομακρυσμένο υπολογιστή.

Η υπηρεσία αυτή χρησιμεύει επίσης για να συνδεθείτε σε μια BBS.

Αυτό το είδος σύνδεσης μπορεί να φανεί εξαιρετικά χρήσιμο για να πάρετε κάποιο αρχείο από το Internet αν έχετε πρόβλημα σύνδεσης μέσω PPP. Αν θέλετε να πάρετε κάτι μέσω FTP και δεν μπορείτε να συνδεθείτε μέσω PPP, συνδεθείτε μέσω τερματικού σε ένα άλλο υπολογιστή, και κατεβάστε σε αυτόν το αρχείο μέσω FTP. Έπειτα, χρησιμοποιήστε το πρωτόκολλο zmodem για να το μεταφέρετε στον υπολογιστή σας.

50.1. Το τύπου Hayes Modem μου δεν Υποστηρίζεται, Τι Μπορώ να Κάνω;

Στην πραγματικότητα, η σελίδα manual της `tip` δεν είναι ενημερωμένη. Υπάρχει ήδη κατάλληλο γενικό πρόγραμμα κλήσης για modems της Hayes. Απλώς χρησιμοποιήστε την καταχώριση `at=hayes` στο αρχείο /etc/remote.

Το πρόγραμμα οδήγησης Hayes δεν είναι αρκετά έξυπνο ώστε να αναγνωρίζει κάποια από τα προχωρημένα χαρακτηριστικά των νεώτερων modems. Μπορεί να μπερδευτεί από μηνύματα όπως τα `BUSY`, `NO DIALTONE`, ή `CONNECT 115200`. Θα πρέπει να απενεργοποιήσετε αυτά τα μηνύματα όταν χρησιμοποιείται την `tip` (στέλνοντας την εντολή `ATX0&W`).

Επίσης, το μέγιστο χρονικό διάστημα το οποίο περιμένει η `tip` είναι 60 δευτερόλεπτα. Το modem σας θα πρέπει να έχει μικρότερο χρονικό περιθώριο, αλλιώς η tip θα νομίζει ότι υπάρχει πρόβλημα επικοινωνίας. Δοκιμάστε την εντολή `ATS7=45&W`.

50.2. Πως Υποτίθεται Ότι θα Στείλω Αυτές τις `AT` Εντολές;

Δημιουργήστε αυτό που ονομάζεται "απευθείας" καταχώριση στο αρχείο /etc/remote. Για παράδειγμα, αν το modem σας είναι συνδεμένο στην πρώτη σειριακή θύρα, /dev/cuau0, προσθέστε την ακόλουθη γραμμή:

```
cuau0:dv=/dev/cuau0:br#19200:pa=none
```

Στην ικανότητα br, χρησιμοποιήστε τον υψηλότερο ρυθμό bps που υποστηρίζει το modem σας.

Έπειτα, πληκτρολογήστε `tip cuau0` και θα συνδεθείτε με το modem σας

Ή χρησιμοποιήστε την `cu` ως `root`, δίνοντας την ακόλουθη εντολή:

```
# cu -lline -sspeed
```

Το *line* είναι η σειριακή θύρα (π.χ. /dev/cuau0) και το *speed* είναι η ταχύτητα (π.χ. `57600`). Όταν τελειώσετε με τις εντολές AT, γράψτε `~.` για να τερματίσετε τη σύνδεση.

50.3. Το Σύμβολο `@` της Ικανότητας pn Δεν Λειτουργεί!

Το σύμβολο `@` της ικανότητας τηλεφωνικού αριθμού (pn, phone number) οδηγεί την tip να διαβάσει το αρχείο /etc/phones για ένα τηλεφωνικό αριθμό. Αλλά το σύμβολο `@` είναι επίσης ένας ειδικός χαρακτήρας σε αρχεία ικανοτήτων όπως το /etc/remote. Θα πρέπει να χρησιμοποιήσετε την ανάποδη κάθετο για να δηλώσετε ότι δεν επιθυμείτε να έχει επίδραση ειδικού χαρακτήρα:

```
pn=\@
```

50.4. Πως Μπορώ να Καλέσω Ένα Τηλεφωνικό Αριθμό Από την Γραμμή Εντολών;

Βάλτε μια "γενική" καταχώριση στο αρχείο /etc/remote. Για παράδειγμα:

```
tip115200|Dial any phone number at 115200 bps:\
        :dv=/dev/cuau0:br#115200:at=hayes:pa=none:du:
tip57600|Dial any phone number at 57600 bps:\
        :dv=/dev/cuau0:br#57600:at=hayes:pa=none:du:
```

Έπειτα μπορείτε να δίνετε εντολές όπως:

```
# tip -115200 5551234
```

Αν προτιμάτε την `cu` αντί για την `tip`, χρησιμοποιήστε μια γενική καταχώριση για την `cu`:

```
cu115200|Use cu to dial any number at 115200bps:\
        :dv=/dev/cuau1:br#57600:at=hayes:pa=none:du:
```

και πληκτρολογήστε:

```
# cu 5551234 -s 115200
```

50.5. Πρέπει να Πληκτρολογώ το Ρυθμό bps Κάθε Φορά που το Κάνω Αυτό;

Θα πρέπει να προσθέσετε μια καταχώριση `tip1200` ή `cu1200`, αλλά μπορείτε να βάλετε την δική σας επιθυμητή τιμή στην ικανότητα br. Η εντολή `tip` θεωρεί ότι τα 1200 bps είναι μια καλή προεπιλογή, και για το λόγο αυτό ψάχνει να βρει μια καταχώριση `tip1200`. Δεν χρειάζεται ωστόσο να χρησιμοποιήσετε ταχύτητα 1200 bps.

50.6. Έχω Πρόσβαση σε Ένα Αριθμό Υπολογιστών Μέσω Ενός Εξυπηρετητή Τερματικών

Αντί να περιμένετε μέχρι να συνδεθείτε και να πληκτρολογείτε `CONNECT host` κάθε φορά, χρησιμοποιήστε την ικανότητα `cm` του tip. Για παράδειγμα, δείτε τις παρακάτω καταχωρίσεις στο /etc/remote:

```
pain|pain.deep13.com|Forrester's machine:\
        :cm=CONNECT pain\n:tc=deep13:
muffin|muffin.deep13.com|Frank's machine:\
        :cm=CONNECT muffin\n:tc=deep13:
deep13:Gizmonics Institute terminal server:\
        :dv=/dev/cuau2:br#38400:at=hayes:du:pa=none:pn=5551234:
```

Το παραπάνω, θα σας επιτρέψει να γράφετε `tip pain` ή `tip muffin` για να συνδέεστε στους υπολογιστές `pain` ή `muffin`, και `tip deep13` για να συνδέεστε στον εξυπηρετητή τερματικών.

50.7. Μπορεί η Tip να Δοκιμάσει Περισσότερες Από Μια Γραμμές για κάθε Σύνδεση;

Αυτό το πρόβλημα συνήθως εμφανίζεται σε ένα πανεπιστήμιο που έχει αρκετές γραμμές για modem, αλλά και χιλιάδες φοιτητές που προσπαθούν να τις χρησιμοποιήσουν.

Δημιουργήστε μια καταχώριση για το πανεπιστήμιο σας στο /etc/remote και χρησιμοποιήστε το `@` στην ικανότητα `pn`:

```
big-university:\
        :pn=\@:tc=dialout
dialout:\
        :dv=/dev/cuau3:br#9600:at=courier:du:pa=none:
```

Έπειτα, δημιουργήστε μια λίστα με τους αριθμούς τηλεφώνων του πανεπιστημίου στο /etc/phones:

```
big-university 5551111
big-university 5551112
big-university 5551113
```

```
big-university 5551114
```

Η `tip` θα δοκιμάσει κάθε μία, με τη σειρά που εμφανίζονται, και θα σταματήσει. Αν θέλετε να συνεχίζει την προσπάθεια, εκτελέστε την `tip` μέσα σε ένα βρόγχο while.

50.8. Γιατί Πρέπει να Πιέσω `Ctrl` + `P` Δύο Φορές για να Στείλω το Συνδυασμό `Ctrl` + `P` Μια Φορά;

Ο συνδυασμός πλήκτρων `Ctrl` + `P` αποτελεί τον προεπιλεγμένο χαρακτήρα "εξαναγκασμού (force)", και χρησιμοποιείται για να καταλάβει η `tip` ότι ο επόμενος χαρακτήρας θα πρέπει να χρησιμοποιηθεί όπως είναι. Μπορείτε να θέσετε τον χαρακτήρα εξαναγκασμού σε οποιοδήποτε άλλο χαρακτήρα, χρησιμοποιώντας την ακολουθία διαφυγής `~s`, η οποία σημαίνει "ρύθμισε μια μεταβλητή".

Πληκτρολογήστε `~sforce=single-char` και συνεχίστε με ένα χαρακτήρα νέας γραμμής. Το *single-char* είναι οποιοσδήποτε μονός χαρακτήρας. Αν αφήσετε κενό το *single-char*, ο χαρακτήρας εξαναγκασμού θα είναι ο nul, τον οποίο μπορείτε να πληκτρολογήσετε χρησιμοποιώντας το συνδυασμό πλήκτρων `Ctrl` + `2` ή `Ctrl` + `Space`. Μια αρκετά καλή τιμή για το *single-char* είναι το `Shift` + `Ctrl` + `6`, που χρησιμοποιείται μόνο σε κάποιους εξυπηρετητές τερματικών.

Μπορείτε να ορίσετε το χαρακτήρα εξαναγκασμού σε όποιον εσείς επιθυμείτε, με την ακόλουθη καταχώριση στο αρχείο $HOME/.tiprc:

```
force=single-char
```

50.9. Ξαφνικά Ότι Γράφω Εμφανίζεται με Κεφαλαία Γράμματα!!

Μάλλον έχετε πιέσει `Ctrl` + `A`, που είναι ο "χαρακτήρας ανύψωσης" της `tip`, και είναι σχεδιασμένος ειδικά για όσους έχουν πρόβλημα με το πλήκτρο `CAPS LOCK`. Χρησιμοποιήστε την εντολή `~s` που δείξαμε παραπάνω, για να θέσετε μια λογική τιμή στη μεταβλητή `raisechar`. Στην πραγματικότητα, μπορείτε να θέσετε την ίδια τιμή με τον χαρακτήρα εξαναγκασμού, αν δεν σκοπεύετε ποτέ να χρησιμοποιήσετε κάποια από αυτές τις δυνατότητες.

Παρακάτω φαίνεται ένα υπόδειγμα αρχείου .tiprc, το οποίο είναι τέλειο για χρήστες του Emacs που χρειάζεται να πληκτρολογούν συχνά `Ctrl` + `2` και `Ctrl` + `A`:

```
force=^^
raisechar=^^
```

Ο χαρακτήρας `^^` είναι ο `Shift` + `Ctrl` + `6`.

50.10. Πως Μπορώ να Μεταφέρω Αρχεία με την `tip`;

Αν επικοινωνείτε με άλλο UNIX® σύστημα, μπορείτε να στείλετε και να λάβετε αρχεία με τις εντολές `~p` (put) και `~t` (take). Οι εντολές αυτές εκτελούν τις cat και echo στο απομακρυσμένο σύστημα για να λαμβάνουν και να στέλνουν αρχεία. Η σύνταξη τους είναι:

`~p` τοπικό-αρχείο [απομακρυσμένο-αρχείο]

`~t` απομακρυσμένο-αρχείο [τοπικό-αρχείο]

Οι παραπάνω εντολές δεν διαθέτουν έλεγχο λαθών. Θα είναι καλύτερο να χρησιμοποιήσετε κάποιο άλλο πρωτόκολλο, όπως το zmodem.

50.11. Πως Μπορώ να Εκτελέσω το zmodem με την `tip`;

Για να λάβετε αρχεία, ξεκινήστε το πρόγραμμα αποστολής στον απομακρυσμένο υπολογιστή. Έπειτα πληκτρολογήστε `~C rz` για να ξεκινήσετε την τοπική λήψη.

Για να στείλετε αρχεία, ξεκινήστε το πρόγραμμα λήψης στον απομακρυσμένο υπολογιστή. Έπειτα πληκτρολογήστε `~C sz files` για να στείλετε τα αρχεία στο απομακρυσμένο σύστημα.

Chapter 51. Ρύθμιση της Σειριακής Κονσόλας

Από το FreeBSD 8.0 και μετά, τα αρχεία συσκευών των σειριακών θυρών μετονομάστηκαν από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν την παρακάτω τεκμηρίωση σύμφωνα με τις παραπάνω αλλαγές.

51.1. Εισαγωγή

Το FreeBSD έχει την ικανότητα να εκκινήσει σε ένα σύστημα το οποίο ως κονσόλα διαθέτει ένα "κουτό" τερματικό συνδεμένο σε μια σειριακή θύρα. Αυτή η ρύθμιση είναι χρήσιμη σε δύο κατηγορίες ανθρώπων: διαχειριστές συστημάτων που επιθυμούν να εγκαταστήσουν FreeBSD σε μηχανήματα τα οποία δεν διαθέτουν πληκτρολόγιο ή οθόνη, και προγραμματιστές που επιθυμούν να εκσφαλματώνουν τον πυρήνα ή οδηγούς συσκευών.

Όπως περιγράφεται στο Η Διαδικασία Εκκίνησης του FreeBSD, το FreeBSD χρησιμοποιεί σύστημα εκκίνησης τριών σταδίων. Τα πρώτα δύο στάδια είναι στον κώδικα του boot block, ο οποίος αποθηκεύεται στην αρχή της κατάτμησης (slice) του δίσκου εκκίνησης του FreeBSD. Το boot block κατόπιν φορτώνει και εκτελεί τον φορτωτή εκκίνησης (/boot/loader) ως κώδικα του τρίτου σταδίου.

Για να ενεργοποιήσετε την σειριακή κονσόλα, θα πρέπει να ρυθμίσετε τον κώδικα του boot block, το φορτωτή εκκίνησης, και τον πυρήνα.

51.2. Ρύθμιση Σειριακής Κονσόλας (Σύντομη Έκδοση)

Η ενότητα αυτή υποθέτει ότι σκοπεύετε να χρησιμοποιήσετε τις προεπιλεγμένες ρυθμίσεις, και θέλετε απλώς μια γρήγορη επισκόπηση της διαδικασίας ρύθμισης της σειριακής κονσόλας.

1. Συνδέστε το σειριακό καλώδιο στην COM1 και στο τερματικό.
2. Για να δείτε όλα τα μηνύματα εκκίνησης στην σειριακή κονσόλα, δώστε την παρακάτω εντολή ως υπερχρήστης:

   ```
   # echo 'console="comconsole"' >> /boot/loader.conf
   ```

3. Επεξεργαστείτε το /etc/ttys και αλλάξτε το `off` σε `on` και το `dialup` σε `vt100` για την καταχώριση ttyu0. Διαφορετικά, δεν θα χρειάζεται κωδικός πρόσβασης για τη σύνδεση μέσω της σειριακής κονσόλας, το οποίο αποτελεί πιθανό κενό ασφαλείας.
4. Επανεκκινήστε το σύστημα για να δείτε αν ίσχυσαν οι αλλαγές.

Αν χρειάζεστε διαφορετικές ρυθμίσεις, θα βρείτε λεπτομέρειες για την ρύθμιση στο Ρύθμιση Σειριακής Κονσόλας.

51.3. Ρύθμιση Σειριακής Κονσόλας

1. Προετοιμάστε ένα σειριακό καλώδιο.

   Θα χρειαστείτε είτε ένα καλώδιο τύπου null-modem, είτε ένα τυποποιημένο σειριακό καλώδιο και ένα προσαρμογέα null-modem. Δείτε το Θύρες και Καλώδια για λεπτομέρειες σχετικά με τα είδη των σειριακών καλωδίων.

2. Αποσυνδέστε το πληκτρολόγιο σας.

   Τα περισσότερα PC ψάχνουν για το πληκτρολόγιο κατά την διάρκεια των διαγνωστικών εκκίνησης (POST, Power On Self Test), και θα αναφέρουν σφάλμα αν το πληκτρολόγιο δεν είναι συνδεμένο. Μερικά μηχανήματα παραπονιούνται ηχηρά για την έλλειψη πληκτρολογίου, και δεν συνεχίζουν την εκκίνηση μέχρι να το συνδέσετε.

   Αν ο υπολογιστής σας παραπονιέται για το λάθος, αλλά ξεκινά έτσι και αλλιώς, δεν χρειάζεται να κάνετε τίποτα ιδιαίτερο για αυτό. (Μερικά μηχανήματα με BIOS της Phoenix, λένε απλώς `Keyboard Failed` και συνεχίζουν την εκκίνηση κανονικά.)

   Αν ο υπολογιστής σας αρνείται να εκκινήσει χωρίς πληκτρολόγιο, θα πρέπει να ρυθμίσετε το BIOS ώστε να αγνοεί το λάθος (αν γίνεται). Συμβουλευτείτε το εγχειρίδιο της μητρικής σας για λεπτομέρειες σχετικά με αυτή τη διαδικασία.

   Ρυθμίστε το πληκτρολόγιο σε "Not installed" στο BIOS. Η ρύθμιση αυτή απλώς αποτρέπει το BIOS από το να ανιχνεύει το πληκτρολόγιο στην εκκίνηση, και δεν πρόκειται να σας εμποδίσει να το χρησιμοποιήσετε κανονικά. Μπορείτε να αφήσετε το πληκτρολόγιο συνδεμένο ακόμα και όταν έχετε ενεργοποιήσει τη ρύθμιση "Not installed". Αν δεν υπάρχει η παραπάνω ρύθμιση στο BIOS, ψάξτε για την επιλογή "Halt on Error". Αλλάξτε τη σε "All but Keyboard" ή ακόμα και σε "No Errors", και θα έχετε το ίδιο αποτέλεσμα.

   Αν το σύστημα σας διαθέτει ποντίκι τύπου PS/2®, πιθανόν να πρέπει να το αποσυνδέσετε και αυτό. Τα ποντίκια τύπου PS/2® έχουν κάποια κυκλώματα κοινά με το πληκτρολόγιο, γεγονός που μπορεί να προκαλέσει σύγχυση στο πρόγραμμα ανίχνευσης του πληκτρολογίου. Κάποια συστήματα, όπως το Gateway 2000 Pentium 90 MHz με AMI BIOS, συμπεριφέρονται με αυτό τον τρόπο. Σε γενικές γραμμές, αυτό δεν είναι πρόβλημα καθώς το ποντίκι έτσι και αλλιώς δεν είναι χρήσιμο χωρίς το πληκτρολόγιο.

3. Συνδέστε ένα κουτό τερματικό στην COM1 (sio0).

   Αν δεν έχετε κουτό τερματικό, μπορείτε να συνδέσετε ένα παλιό PC/XT με ένα πρόγραμμα για modem, ή να χρησιμοποιήσετε τη σειριακή θύρα σε ένα άλλο μηχάνημα UNIX®. Αν δεν έχετε σειριακή θύρα COM1 (sio0), αγοράστε μια. Τη δεδομένη στιγμή δεν υπάρχει τρόπος να επιλέξετε άλλη θύρα εκτός από την COM1, χωρίς να επαναμεταγλωττίσετε τα boot blocks. Αν χρησιμοποιείτε ήδη την COM1 για κάποια άλλη συσκευή, θα πρέπει να την αφαιρέσετε

προσωρινά, και να εγκαταστήσετε νέο boot block και πυρήνα, μόλις συνδεθείτε στο FreeBSD. (Υποθέτουμε ότι η COM1 θα είναι έτσι και αλλιώς διαθέσιμη σε ένα εξυπηρετητή αρχείων/υπολογισμών/τερματικών. Αν πραγματικά χρειάζεστε την COM1 για κάτι άλλο (και δεν μπορείτε αυτό το κάτι άλλο να το μετακινήσετε στην COM2 (sio1)), μάλλον δεν θα έπρεπε να ασχοληθείτε καθόλου με όλο αυτό το θέμα).

4. Βεβαιωθείτε ότι το αρχείο ρυθμίσεων του πυρήνα σας έχει τις κατάλληλες επιλογές (flags) για την COM1 (sio0).

   Οι σχετικές επιλογές είναι:

   `0x10`

   Ενεργοποιεί την υποστήριξη κονσόλας για αυτή τη θύρα. Αν δεν τεθεί αυτή η επιλογή, τα υπόλοιπα flags για την κονσόλα δεν λαμβάνονται υπόψιν. Τη δεδομένη στιγμή, η υποστήριξη κονσόλας μπορεί να είναι ενεργοποιημένη μόνο σε μια θύρα. Η πρώτη που καθορίζεται στο αρχείο ρυθμίσεων, είναι και αυτή που θα προτιμηθεί. Από μόνη της, η επιλογή αυτή δεν θα ενεργοποιήσει την κονσόλα στη συγκεκριμένη σειριακή θύρα. Θα πρέπει να θέσετε το παρακάτω flag ή να χρησιμοποιήσετε την επιλογή `-h` που περιγράφεται παρακάτω, μαζί με αυτό το flag.

   `0x20`

   Εξαναγκάζει τη συγκεκριμένη θύρα να γίνει η κονσόλα (εκτός αν υπάρχει άλλη κονσόλα υψηλότερης προτεραιότητας) άσχετα με την επιλογή `-h` που περιγράφεται παρακάτω. Θα πρέπει να χρησιμοποιήσετε το flag `0x20` μαζί με το flag `0x10`.

   `0x40`

   Παρακρατεί τη συγκεκριμένη θύρα (σε συνδυασμό με την `0x10`) κάνοντας την μη διαθέσιμη για κανονική πρόσβαση. Δεν θα πρέπει να θέσετε αυτή την επιλογή στη σειριακή θύρα που σκοπεύετε να χρησιμοποιήσετε ως σειριακή κονσόλα. Η μόνη χρήση αυτού του flag, είναι να καθορίσετε ότι η θύρα θα χρησιμοποιηθεί για απομακρυσμένη εκσφαλμάτωση του πυρήνα (kernel debugging). Δείτε Το Βιβλίο του Προγραμματιστή για περισσότερες λεπτομέρειες σχετικά με την απομακρυσμένη εκσφαλμάτωση.

   Παράδειγμα:

   ```
   device sio0 flags 0x10
   ```

   Δείτε τη σελίδα manual sio(4) για περισσότερες λεπτομέρειες.

   Αν δεν έχουν καθοριστεί flags, θα πρέπει να εκτελέσετε το UserConfig (σε διαφορετική κονσόλα) ή να επαναμεταγλωττίσετε τον πυρήνα.

5. Δημιουργήστε το αρχείο boot.config στον ριζικό κατάλογο της κατάτμησης `a` του δίσκου εκκίνησης.

   Το αρχείο αυτό θα κατευθύνει τον κώδικα του boot block σχετικά με το πως θέλετε να εκκινήσει το σύστημα. Για να ενεργοποιήσετε την σειριακή κονσόλα, θα χρειαστείτε μία ή περισσότερες από τις παρακάτω επιλογές-αν θέλετε να προσδιορίσετε πολλαπλές επιλογές,

θα πρέπει να τις περιλάβετε όλες στην ίδια γραμμή.

`-h`

Εναλλάσσει μεταξύ της εσωτερικής και της σειριακής κονσόλας. Για παράδειγμα, αν ξεκινήσετε από την εσωτερική κονσόλα (οθόνη), μπορείτε να χρησιμοποιήσετε την επιλογή `-h` για να κατευθύνετε το φορτωτή εκκίνησης και τον πυρήνα να χρησιμοποιήσουν τη σειριακή θύρα ως συσκευή κονσόλας. Εναλλακτικά, αν εκκινήσετε μέσω της σειριακής θύρας, μπορείτε να χρησιμοποιήσετε την επιλογή `-h` για να κατευθύνετε το φορτωτή εκκίνησης και τον πυρήνα να χρησιμοποιήσουν την κανονική κονσόλα αντί για τη σειριακή.

`-D`

Εναλλάσσει μεταξύ της απλής και της διπλής κονσόλας. Στην ρύθμιση απλής κονσόλας, θα χρησιμοποιηθεί είτε η εσωτερική κονσόλα (απεικόνιση σε οθόνη) είτε η σειριακή θύρα, ανάλογα με το πως έχει τεθεί η επιλογή `-h` που εξετάσαμε παραπάνω. Σε περίπτωση διπλής κονσόλας, θα ενεργοποιηθούν ταυτόχρονα τόσο η εσωτερική όσο και η σειριακή κονσόλα, άσχετα από τη ρύθμιση της επιλογής `-h`. Σημειώστε ωστόσο ότι η ρύθμιση διπλής κονσόλας μπορεί να ενεργοποιηθεί μόνο κατά την εκκίνηση, όσο εκτελείται το boot block. Μόλις δοθεί ο έλεγχος στο φορτωτή εκκίνησης, η μοναδική κονσόλα που παραμένει είναι αυτή που καθορίζεται από την επιλογή `-h`.

`-P`

Ενεργοποιεί την ανίχνευση πληκτρολογίου του boot block. Αν δεν βρεθεί πληκτρολόγιο, ενεργοποιούνται αυτόματα οι επιλογές `-D` και `-h`.

Λόγω περιορισμών χώρου στην τρέχουσα έκδοση των boot blocks, η επιλογή `-P` μπορεί να ανιχνεύσει μόνο εκτεταμένα (extended) πληκτρολόγια. Πληκτρολόγια με λιγότερα από 101 πλήκτρα (και χωρίς τα πλήκτρα `F11` και `F12`) ίσως να μην ανιχνευθούν. Εξαιτίας αυτού του περιορισμού, είναι πιθανό να μην ανιχνευθούν και κάποια πληκτρολόγια φορητών υπολογιστών. Αν συμβαίνει αυτό στο σύστημα σας, θα πρέπει να σταματήσετε να χρησιμοποιείτε την επιλογή `-P`. Δυστυχώς, δεν υπάρχει κάποιος τρόπος να παρακάμψετε αυτό το πρόβλημα.

Χρησιμοποιήστε είτε την επιλογή `-P` για να επιλέξετε την κονσόλα αυτόματα, ή την επιλογή `-h` για να ενεργοποιήσετε τη σειριακή κονσόλα.

Μπορείτε επίσης να περιλάβετε και άλλες επιλογές που περιγράφονται στη σελίδα manual του boot(8).

Όλες οι επιλογές εκκίνησης, εκτός της `-P`, θα περάσουν στο φορτωτή εκκίνησης (/boot/loader). Ο φορτωτής εκκίνησης θα καθορίσει αν η κονσόλα θα δημιουργηθεί στην οθόνη ή στη σειριακή θύρα, αφού εξετάσει μόνο την επιλογή `-h`. Αυτό σημαίνει ότι αν καθορίσετε την επιλογή `-D` αλλά όχι την επιλογή `-h` στο /boot.config, θα μπορείτε να χρησιμοποιήσετε την σειριακή θύρα ως κονσόλα μόνο κατά την εκτέλεση του boot block. Ο φορτωτής εκκίνησης όμως θα χρησιμοποιήσει την εσωτερική κονσόλα (οθόνη).

6. Εκκινήστε το μηχάνημα.

   Όταν ξεκινήσετε το FreeBSD μηχάνημα, τα boot blocks θα δείξουν τα περιεχόμενα του /boot.config στην κονσόλα. Για παράδειγμα:

   ```
   /boot.config: -P
   Keyboard: no
   ```

   Η δεύτερη γραμμή θα εμφανιστεί μόνο αν βάλετε την επιλογή `-P` στο /boot.config, και δείχνει αν υπάρχει ή όχι συνδεμένο πληκτρολόγιο. Τα μηνύματα αυτά κατευθύνονται στην σειριακή ή στην εσωτερική κονσόλα, ή ακόμα και στις δύο, ανάλογα με την επιλογή που έχει γίνει στο /boot.config.

Επιλογές	**Το μήνυμα εμφανίζεται στην**
καμία	εσωτερική κονσόλα
`-h`	σειριακή κονσόλα
`-D`	εσωτερική και σειριακή κονσόλα
`-Dh`	σειριακή και εσωτερική κονσόλα
`-P`, πληκτρολόγιο συνδεμένο	εσωτερική κονσόλα
`-P`, χωρίς πληκτρολόγιο	σειριακή κονσόλα

   Μετά τα παραπάνω μηνύματα, θα υπάρξει μια μικρή παύση πριν τα boot blocks συνεχίσουν φορτώνοντας το φορτωτή εκκίνησης, και πριν εμφανιστούν περισσότερα μηνύματα στην κονσόλα. Υπό κανονικές συνθήκες, δεν χρειάζεται να διακόψετε τα boot blocks, αλλά ίσως θέλετε να το κάνετε αυτό για να βεβαιωθείτε ότι όλα είναι ρυθμισμένα σωστά.

   Πιέστε οποιοδήποτε πλήκτρο εκτός από το `Enter` στην κονσόλα για να διακόψετε τη διαδικασία εκκίνησης. Τα boot blocks θα σας ρωτήσουν για περισσότερες πληροφορίες. Θα πρέπει να δείτε κάτι όπως το παρακάτω:

   ```
   >> FreeBSD/i386 BOOT
   Default: 0:ad(0,a)/boot/loader
   boot:
   ```

   Επαληθεύστε ότι το παραπάνω μήνυμα εμφανίζεται είτε στη σειριακή κονσόλα, ή στην εσωτερική κονσόλα ή και στις δύο, ανάλογα με τις επιλογές που έχετε βάλει στο αρχείο /boot.config. Αν το μήνυμα εμφανίζεται στην σωστή κονσόλα, πιέστε `Enter` για να συνεχίσετε με τη διαδικασία εκκίνησης.

   Αν επιθυμείτε σειριακή κονσόλα, αλλά δεν βλέπετε την προτροπή σε αυτήν, υπάρχει κάποιο λάθος στις ρυθμίσεις. Στο μεταξύ, γράψτε `-h` και πιέστε `Enter` ή `Return` (αν γίνεται) για να πείτε στο boot block (και έπειτα στο φορτωτή εκκίνησης και τον πυρήνα) να επιλέξει τη σειριακή θύρα για την κονσόλα. Μόλις το σύστημα ξεκινήσει, κοιτάξτε ξανά τις ρυθμίσεις για να βρείτε που είναι το λάθος.

Μετά τη φόρτωση του φορτωτή εκκίνησης, βρίσκεστε στο τρίτο στάδιο της διαδικασίας εκκίνησης και έχετε ακόμα τη δυνατότητα να επιλέξετε μεταξύ της εσωτερικής και σειριακής κονσόλας, θέτοντας τις κατάλληλες μεταβλητές περιβάλλοντος στο φορτωτή εκκίνησης. Δείτε το Αλλαγή Κονσόλας μέσω του Φορτωτή Εκκίνησης.

51.4. Περίληψη

Εδώ θα βρείτε μια περίληψη των διάφορων επιλογών που παρουσιάστηκαν σε αυτή την ενότητα, και την κονσόλα που επιλέχθηκε τελικά.

51.4.1. 1η Περίπτωση: Έχετε Θέσει το Flag 0x10 για τη Θύρα sio0

```
device sio0 flags 0x10
```

Επιλογές στο /boot.config	Κονσόλα κατά τη διάρκεια των boot blocks	Κονσόλα κατά τη διάρκεια του φορτωτή εκκίνησης	Κονσόλα στον πυρήνα
καμία	εσωτερική	εσωτερική	εσωτερική
-h	σειριακή	σειριακή	σειριακή
-D	σειριακή και εσωτερική	εσωτερική	εσωτερική
-Dh	σειριακή και εσωτερική	σειριακή	σειριακή
-P, πληκτρολόγιο συνδεμένο	εσωτερική	εσωτερική	εσωτερική
-P, χωρίς πληκτρολόγιο	σειριακή και εσωτερική	σειριακή	σειριακή

51.4.2. 2η Περίπτωση: Έχετε Θέσει το Flag 0x30 για την Θύρα sio0

```
device sio0 flags 0x30
```

Επιλογές στο /boot.config	Κονσόλα κατά τη διάρκεια των boot blocks	Κονσόλα κατά τη διάρκεια του φορτωτή εκκίνησης	Κονσόλα στον πυρήνα
καμία	εσωτερική	εσωτερική	σειριακή
-h	σειριακή	σειριακή	σειριακή
-D	σειριακή και εσωτερική	εσωτερική	σειριακή
-Dh	σειριακή και εσωτερική	σειριακή	σειριακή
-P, πληκτρολόγιο συνδεμένο	εσωτερική	εσωτερική	σειριακή
-P, χωρίς πληκτρολόγιο	σειριακή και εσωτερική	σειριακή	σειριακή

51.5. Συμβουλές για την Σειριακή Κονσόλα

51.5.1. Ρύθμιση Μεγαλύτερης Ταχύτητας για τη Σειριακή Θύρα

Οι προεπιλεγμένες ρυθμίσεις της σειριακής θύρας είναι: 9600 baud, 8 bits, χωρίς ισοτιμία (parity), 1 stop bit. Αν θέλετε να αλλάξετε την προεπιλεγμένη ταχύτητα της κονσόλας, έχετε τις παρακάτω επιλογές:

- Επαναμεταγλωττίστε τα boot blocks θέτοντας τη μεταβλητή `BOOT_COMCONSOLE_SPEED` για να ορίσετε την νέα ταχύτητα κονσόλας. Δείτε το Χρησιμοποιώντας Σειριακή Θύρα Εκτός της sio0 για την Κονσόλα. για λεπτομερείς οδηγίες σχετικά με τη μεταγλώττιση και εγκατάσταση νέων boot blocks.

  Αν η ενεργοποίηση της σειριακής κονσόλας δεν γίνεται μέσω της επιλογής `-h`, ή αν η σειριακή κονσόλα που χρησιμοποιείται από τον πυρήνα είναι διαφορετική από αυτή που χρησιμοποιείται από τα boot blocks, θα πρέπει επίσης να προσθέσετε την παρακάτω επιλογή στο αρχείο ρυθμίσεων του πυρήνα, και να μεταγλωττίσετε ένα νέο πυρήνα:

  ```
  options CONSPEED=19200
  ```

- Στις επιλογές εκκίνησης του πυρήνα, χρησιμοποιήστε το `-S`. Μπορείτε επίσης να προσθέσετε την επιλογή `-S` στο /boot.config. Η σελίδα manual boot(8) περιέχει μια λίστα των υποστηριζόμενων επιλογών, και περιγράφει πως να τις προσθέσετε στο αρχείο /boot.config.
- Ενεργοποιήστε την επιλογή `comconsole_speed` στο αρχείο /boot/loader.conf.

  Για να λειτουργήσει αυτή η επιλογή, θα πρέπει επίσης να θέσετε τιμές για τις επιλογές `console`, `boot_serial`, και `boot_multicons` στο ίδιο αρχείο, το /boot/loader.conf. Παρακάτω φαίνεται ένα παράδειγμα χρήσης του `comconsole_speed` για αλλαγή ταχύτητα της σειριακής κονσόλας:

  ```
  boot_multicons="YES"
  boot_serial="YES"
  comconsole_speed="115200"
  console="comconsole,vidconsole"
  ```

51.5.2. Χρησιμοποιώντας Σειριακή Θύρα Εκτός της sio0 για την Κονσόλα.

Θα πρέπει να επαναμεταγλωττίσετε κάποια προγράμματα για να χρησιμοποιήσετε ως κονσόλα μια σειριακή θύρα εκτός της sio0. Αν για οποιοδήποτε λόγο θέλετε να χρησιμοποιήσετε άλλη σειριακή θύρα, θα πρέπει να επαναμεταγλωττίσετε τα boot blocks, το φορτωτή εκκίνησης και τον πυρήνα, με τον τρόπο που φαίνεται παρακάτω.

1. Ανακτήστε τον πηγαίο κώδικα του πυρήνα. (Δείτε το Ενημέρωση και Αναβάθμιση του FreeBSD)
2. Επεξεργαστείτε το αρχείο /etc/make.conf και θέστε την επιλογή `BOOT_COMCONSOLE_PORT` στη διεύθυνση της θύρας που θέλετε να χρησιμοποιήσετε (0x3F8, 0x2F8, 0x3E8 or 0x2E8). Μπορείτε να χρησιμοποιήσετε μόνο τις θύρες sio0 ως sio3 (COM1 ως COM4). Κάρτες πολλαπλών θυρών, δεν πρόκειται να λειτουργήσουν. Δεν χρειάζεται να ρυθμίσετε την τιμή του interrupt.

3. Δημιουργήστε ένα αρχείο ρύθμισης προσαρμοσμένου πυρήνα, και προσθέστε τα κατάλληλα flags για τη σειριακή θύρα που επιθυμείτε να χρησιμοποιήσετε. Για παράδειγμα, αν θέλετε η sio1 (COM2) να γίνει η κονσόλα:

   ```
   device sio1 flags 0x10
   ```

   ή

   ```
   device sio1 flags 0x30
   ```

   Δεν θα πρέπει να θέσετε flags κονσόλας για τις άλλες σειριακές θύρες.

4. Μεταγλωττίστε και εγκαταστήστε ξανά τα boot blocks και τον φορτωτή εκκίνησης:

   ```
   # cd /sys/boot
   # make clean
   # make
   # make install
   ```

5. Επαναμεταγλωττίστε και εγκαταστήστε τον πυρήνα.
6. Γράψτε τα boot blocks στον δίσκο εκκίνησης χρησιμοποιώντας την bsdlabel(8) και εκκινήστε με το νέο πυρήνα.

51.5.3. Είσοδος στον DDB Debugger Μέσω της Σειριακής Γραμμής

Αν θέλετε να εισέλθετε στον debugger του πυρήνα από την σειριακή κονσόλα (κάτι που είναι χρήσιμο για να εκτελέσετε διαγνωστικά από απομακρυσμένη τοποθεσία, αλλά επίσης και επικίνδυνο αν στείλετε κατά λάθος BREAK μέσω της σειριακής θύρας!) θα πρέπει να περιλάβετε την παρακάτω επιλογή στον πυρήνα σας:

```
options BREAK_TO_DEBUGGER
options DDB
```

51.5.4. Προτροπή Εισόδου στην Σειριακή Κονσόλα

Αν και αυτό δεν είναι απαραίτητο, ίσως να θέλετε να έχετε προτροπή εισόδου (*login*) μέσω της σειριακής γραμμής, τώρα που μπορείτε πλέον να δείτε τα μηνύματα εκκίνησης και να εισέλθετε στο debugger του πυρήνα μέσω της σειριακής κονσόλας. Η διαδικασία περιγράφεται παρακάτω.

Με κάποιο συντάκτη κειμένου, ανοίξτε το αρχείο /etc/ttys και βρείτε τις γραμμές:

```
ttyu0 "/usr/libexec/getty std.9600" unknown off secure
ttyu1 "/usr/libexec/getty std.9600" unknown off secure
ttyu2 "/usr/libexec/getty std.9600" unknown off secure
```

```
ttyu3 "/usr/libexec/getty std.9600" unknown off secure
```

Οι καταχωρίσεις από ttyu0 ως ttyu3 αντιστοιχούν στις COM1 ως COM4. Αλλάξτε το `off` σε `on` για την θύρα που επιθυμείτε. Αν έχετε αλλάξει την ταχύτητα της σειριακής θύρας, θα χρειαστεί να αλλάξετε το `std.9600` ώστε να ταιριάζει με την τρέχουσα ρύθμιση, π.χ. `std.19200`.

Μάλλον θα θέλετε να αλλάξετε και τον τύπο του τερματικού, από `unknown` στον πραγματικό τύπου του σειριακού σας τερματικού.

Αφού αλλάξετε τις ρυθμίσεις, θα πρέπει να εκτελέσετε την εντολή `kill -HUP 1` ώστε να ενεργοποιηθούν.

51.6. Αλλαγή Κονσόλας μέσω του Φορτωτή Εκκίνησης

Σε προηγούμενες ενότητες, περιγράψαμε πως να ρυθμίσετε την σειριακή κονσόλα αλλάζοντας τις ρυθμίσεις του boot block. Στην ενότητα αυτή, δείχνουμε πως μπορείτε να καθορίσετε την κονσόλα δίνοντας κάποιες εντολές και μεταβλητές περιβάλλοντος στον φορτωτή εκκίνησης. Καθώς ο φορτωτής εκκίνησης καλείται από το τρίτο στάδιο της διαδικασίας εκκίνησης, και μετά το boot block, οι ρυθμίσεις του φορτωτή εκκίνησης υπερισχύουν σε σχέση με αυτές του boot block.

51.6.1. Ρύθμιση της Σειριακής Κονσόλας

Μπορείτε εύκολα να καθορίσετε ότι θα χρησιμοποιηθεί η σειριακή κονσόλα στον φορτωτή εκκίνησης και στον πυρήνα που θα φορτωθεί, γράφοντας απλώς μια γραμμή στο /boot/loader.conf:

```
console="comconsole"
```

Η ρύθμιση αυτή θα ενεργοποιηθεί, άσχετα με το boot block που συζητήσαμε στην προηγούμενη ενότητα.

Είναι καλύτερα η γραμμή αυτή να είναι η πρώτη στο αρχείο /boot/loader.conf, ώστε να βλέπετε τα αρχικά μηνύματα εκκίνησης στη σειριακή κονσόλα.

Με τον ίδιο τρόπο, μπορείτε να καθορίσετε την εσωτερική κονσόλα ως:

```
console="vidconsole"
```

Αν δεν καθορίσετε τη μεταβλητή περιβάλλοντος `console`, ο φορτωτής εκκίνησης (και έπειτα ο πυρήνας) θα χρησιμοποιήσουν οποιαδήποτε κονσόλα έχετε καθορίσει στο boot block με την επιλογή `-h`.

Μπορείτε να καθορίσετε την κονσόλα στο /boot/loader.conf.local ή στο /boot/loader.conf.

Δείτε το loader.conf(5) για περισσότερες πληροφορίες.

Τη δεδομένη στιγμή, ο φορτωτής εκκίνησης δεν έχει επιλογή αντίστοιχη με την `-P` του boot block, και δεν υπάρχει κάποιος τρόπος να γίνει αυτόματη επιλογή μεταξύ

εσωτερικής και σειριακής κονσόλας ανάλογα με την παρουσία πληκτρολογίου.

51.6.2. Χρήση Σειριακής Θύρας Εκτός της sio0 για την Κονσόλα

Θα πρέπει να επαναμεταγλωττίσετε το φορτωτή εκκίνησης ώστε να χρησιμοποιήσει μια σειριακή θύρα διαφορετική από την sio0 για τη σειριακή κονσόλα. Ακολουθήστε τη διαδικασία που περιγράφεται στο Χρησιμοποιώντας Σειριακή Θύρα Εκτός της sio0 για την Κονσόλα..

51.7. Πιθανές Παγίδες

Η γενική ιδέα είναι να επιτρέπεται σε όσους το επιθυμούν, να δημιουργήσουν εξειδικευμένους εξυπηρετητές που δεν απαιτούν κάρτες γραφικών και πληκτρολόγια. Δυστυχώς, αν και τα περισσότερα συστήματα θα σας επιτρέψουν να εκκινήσετε χωρίς πληκτρολόγιο, σε πολύ λίγα θα μπορέσετε να εκκινήσετε χωρίς κάρτα γραφικών. Τα μηχανήματα με BIOS της AMI μπορούν να ρυθμιστούν με αυτό τον τρόπο, αλλάζοντας την επιλογή "graphics adapter" στις ρυθμίσεις του CMOS σε "Not installed."

Τα περισσότερα μηχανήματα ωστόσο δεν υποστηρίζουν αυτή την επιλογή, και θα αρνηθούν να εκκινήσουν αν δεν βάλετε μια κάρτα γραφικών. Στα μηχανήματα αυτά θα πρέπει να αφήσετε μια στοιχειώδη (ακόμα και μονόχρωμη) κάρτα γραφικών, αν και δεν είναι απαραίτητο να συνδέσετε και οθόνη. Μπορείτε επίσης να δοκιμάσετε να εγκαταστήσετε BIOS της AMI.

Chapter 52. PPP

52.1. Σύνοψη

Το FreeBSD διαθέτει πλήθος τρόπων για τη σύνδεση ενός υπολογιστή με ένα άλλο. Για να επιτύχετε σύνδεση μέσω modem στο Internet ή σε ένα άλλο δίκτυο, ή για να επιτρέψετε σε άλλους να συνδεθούν μέσω του συστήματος σας, απαιτείται η χρήση PPP ή SLIP. Το κεφάλαιο αυτό περιγράφει λεπτομερώς τον τρόπο ρύθμισης των παραπάνω υπηρεσιών για χρήση μέσω modem.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να ρυθμίσετε το PPP χρήστη (User PPP).
- Πως να ρυθμίσετε το PPP πυρήνα (Kernel PPP, μόνο για FreeBSD 7.X).
- Πως να ρυθμίσετε το PPPoE (PPP μέσω Ethernet).
- Πως να ρυθμίσετε το PPPoA (PPP μέσω ATM).
- Πως να ρυθμίσετε ένα πελάτη και εξυπηρετητή SLIP (μόνο για FreeBSD 7.X).

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να είστε εξοικειωμένος με τη βασική ορολογία των δικτύων.
- Να κατανοείτε τις βασικές έννοιες και το σκοπό των επιλογικών συνδέσεων και του PPP και/ή SLIP.

Μπορεί να αναρωτιέστε ποια είναι η βασική διαφορά μεταξύ του PPP χρήστη και του PPP πυρήνα. Η απάντηση είναι απλή: το PPP χρήστη επεξεργάζεται τα δεδομένα εισόδου και εξόδου μέσω προγραμμάτων χρήστη (userland) αντί διαμέσου του πυρήνα του λειτουργικού. Αυτό προκαλεί κάποιες επιβαρύνσεις λόγω της αντιγραφής δεδομένων μεταξύ του πυρήνα και της εφαρμογής χρήστη, αλλά επιτρέπει κατά πολύ πιο πλούσια (από άποψη δυνατοτήτων) υλοποίηση του PPP πρωτοκόλλου. Το PPP χρήστη χρησιμοποιεί τη συσκευή tun για την επικοινωνία με τον έξω κόσμο, ενώ το PPP πυρήνα χρησιμοποιεί την συσκευή ppp.

Σε όλο το κεφάλαιο, το PPP χρήστη θα αναφέρεται απλά ως ppp εκτός και αν χρειάζεται να γίνει διάκριση σε σχέση με άλλο λογισμικό PPP όπως το pppd (μόνο για το FreeBSD 7.X). Εκτός αν αναφέρεται διαφορετικά, όλες οι εντολές που εξηγούνται στο κεφάλαιο αυτό θα πρέπει να εκτελούνται ως `root`.

52.2. Χρησιμοποιώντας το PPP Χρήστη

Από το FreeBSD 8.0 και μετά, τα ονόματα συσκευών για τις σειριακές θύρες μετονομάστηκαν από /dev/cuadN σε /dev/cuauN και από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα χρειαστεί να προσαρμόσουν τις παρακάτω οδηγίες σύμφωνα με αυτές τις αλλαγές.

52.2.1. PPP Χρήστη

52.2.1.1. Προϋποθέσεις

Το κείμενο αυτό προϋποθέτει ότι έχετε τα παρακάτω:

- Λογαριασμό σε κάποιο Παροχέα Υπηρεσιών Internet (ISP) στον οποίο συνδέεστε χρησιμοποιώντας PPP.
- Ένα modem ή άλλη συσκευή συνδεμένη στο σύστημα σας, και ρυθμισμένη σωστά ώστε να σας επιτρέπει να συνδεθείτε στον ISP σας.
- Τους αριθμούς κλήσης για τον ISP σας.
- Το όνομα χρήστη (login) και τον κωδικό σας (password). Είτε κανονικό όνομα και κωδικό (τύπου UNIX®) ή ένα ζεύγος ονόματος / κωδικού τύπου PAP ή CHAP.
- Τις IP διευθύνσεις ενός ή περισσότερων διακομιστών ονομάτων (DNS). Φυσιολογικά, ο ISP σας θα σας δώσει δύο τέτοιες διευθύνσεις. Αν δεν έχετε τουλάχιστον μία, μπορείτε να ενεργοποιήσετε την εντολή `enable dns` στο ppp.conf και το ppp θα ρυθμίσει τους διακομιστές ονομάτων για σας. Το χαρακτηριστικό αυτό εξαρτάται από την υποστήριξη της διαπραγμάτευσης DNS από τον ISP σας.

Ο ISP σας ενδεχομένως να σας δώσει και τις παρακάτω πληροφορίες, αλλά δεν είναι εντελώς απαραίτητες:

- Τη διεύθυνση IP για την πύλη (gateway) του ISP σας. Η πύλη είναι το μηχάνημα μέσω του οποίου συνδέεστε, και θα αποτελέσει την *προεπιλεγμένη διαδρομή* (default route) για το μηχάνημα σας. Αν δεν έχετε αυτή την πληροφορία, θα χρησιμοποιηθεί μια εικονική, και όταν συνδεθείτε θα λάβετε την κανονική διεύθυνση από τον διακομιστή PPP του ISP σας.

  Αυτή η διεύθυνση IP αναφέρεται ως `HISADDR` από το ppp.

- Τη μάσκα δικτύου (netmask) που πρέπει να χρησιμοποιήσετε. Αν ο ISP σας δε σας την παρέχει, μπορείτε με ασφάλεια να χρησιμοποιήσετε την τιμή `255.255.255.255`.
- Αν ο ISP σας παρέχει στατική διεύθυνση και όνομα υπολογιστή (hostname) μπορείτε να χρησιμοποιήσετε αυτά. Διαφορετικά, θα αφήσουμε τον απομακρυσμένο υπολογιστή να δώσει όποια διεύθυνση IP θεωρεί κατάλληλη.

Αν σας λείπουν κάποιες από τις απαιτούμενες πληροφορίες, επικοινωνήστε με τον ISP σας.

Σε ολόκληρη την παρούσα ενότητα, πολλά από τα παραδείγματα που δείχνουν τα περιεχόμενα των αρχείων ρυθμίσεων, είναι αριθμημένα ανά γραμμή. Οι αριθμοί αυτοί εξυπηρετούν στην παρουσίαση και τη συζήτηση του κάθε παραδείγματος, και δεν πρέπει να γραφούν μέσα στο πραγματικό αρχείο. Είναι επίσης σημαντικό να τηρείτε η σωστή στοίχιση σε κάθε αρχείο, με τη χρήση στηλοθετών (tabs) και κενών διαστημάτων.

52.2.1.2. Αυτόματη Ρύθμιση PPP

Τόσο το `ppp` όσο και το `pppd` (η υλοποίηση του PPP σε επίπεδο πυρήνα, μόνο στο FreeBSD 7.X)

χρησιμοποιούν τα αρχεία ρυθμίσεων στον κατάλογο /etc/ppp. Μπορείτε να βρείτε παραδείγματα για το ppp χρήστη στον κατάλογο /usr/shared/examples/ppp/.

Η ρύθμιση του ppp απαιτεί την τροποποίηση ενός αριθμού από αρχεία, ανάλογα με τις απαιτήσεις σας. Το τι θα βάλετε σε αυτά, εξαρτάται σε ένα ποσοστό από το αν ο ISP σας αποδίδει στατικές διευθύνσεις IP (δηλ. σας παρέχει μια διεύθυνση IP η οποία δεν αλλάζει) ή δυναμικές (δηλ. η IP διεύθυνση σας αλλάζει κάθε φορά που συνδέεστε στον ISP σας).

52.2.1.2.1. PPP και Στατικές Διευθύνσεις IP

Θα χρειαστεί να τροποποιήσετε το αρχείο ρυθμίσεων /etc/ppp/ppp.conf. Θα πρέπει να μοιάζει με αυτό που φαίνεται παρακάτω:

Οι γραμμές που τελειώνουν με : ξεκινούν στην πρώτη στήλη (αρχή της γραμμής) - όλες οι άλλες γραμμές θα πρέπει να στοιχισθούν με τον τρόπο που φαίνεται, με τη χρήση κενών ή στηλοθετών.

```
1     default:
2       set log Phase Chat LCP IPCP CCP tun command
3       ident user-ppp VERSION (built COMPILATIONDATE)
4       set device /dev/cuau0
5       set speed 115200
6       set dial "ABORT BUSY ABORT NO\\sCARRIER TIMEOUT 5 \
7                 \"\" AT OK-AT-OK ATE1Q0 OK \\dATDT\\T TIMEOUT 40 CONNECT"
8       set timeout 180
9       enable dns
10
11    provider:
12      set phone "(123) 456 7890"
13      set authname foo
14      set authkey bar
15      set login "TIMEOUT 10 \"\" \"\" gin:--gin: \\U word: \\P col: ppp"
16      set timeout 300
17      set ifaddr x.x.x.x y.y.y.y 255.255.255.255 0.0.0.0
18      add default HISADDR
```

Γραμμή 1

Αναγνωρίζει την προεπιλεγμένη καταχώριση. Οι εντολές σε αυτή την καταχώριση εκτελούνται αυτόματα, όταν εκτελείται το ppp.

Γραμμή 2

Ενεργοποιεί την καταγραφή (logging) των παραμέτρων. Όταν οι ρυθμίσεις που έχουν γίνει λειτουργούν ικανοποιητικά, η γραμμή αυτή θα πρέπει να μικρύνει στην παρακάτω:

```
set log phase tun
```

για να αποφευχθούν μεγάλα μεγέθη στα αρχεία καταγραφής.

Γραμμή 3

Λέει στο PPP πως να αναφέρει πληροφορίες για τον εαυτό του στην άλλη μεριά της σύνδεσης. Η διαδικασία αυτή γίνεται αν το PPP έχει πρόβλημα στην διαπραγμάτευση και ολοκλήρωση της σύνδεσης, παρέχοντας με αυτό τον τρόπο πληροφορίες στον απομακρυσμένο διαχειριστή. Οι πληροφορίες αυτές μπορεί να είναι χρήσιμες στην επίλυση του προβλήματος.

Γραμμή 4

Αναγνωρίζει τη συσκευή στην οποία είναι συνδεμένο το modem. Η συσκευή COM1 είναι η /dev/cuau0 και η COM2 είναι η /dev/cuau1.

Γραμμή 5

Καθορίζει την ταχύτητα με την οποία επιθυμείτε να συνδεθείτε. Αν δεν λειτουργεί η τιμή 115200 (η οποία πρέπει να λειτουργεί με κάθε σχετικά σύγχρονο modem), δοκιμάστε με 38400.

Γραμμές 6 & 7

Το αλφαριθμητικό που θα χρησιμοποιηθεί για την κλήση. Το PPP χρήστη χρησιμοποιεί σύνταξη expect-send παρόμοια με αυτή που χρησιμοποιεί το πρόγραμμα chat(8). Δείτε τη σελίδα manual για πληροφορίες σχετικά με τις δυνατότητες αυτής της γλώσσας.

Σημειώστε ότι αυτή η εντολή συνεχίζει στην επόμενη γραμμή για λόγους αναγνωσιμότητας. Αυτό μπορεί να γίνει σε κάθε εντολή του ppp.conf, εφόσον το `\` είναι ο τελευταίος χαρακτήρας της γραμμής.

Γραμμή 8

Καθορίζει το χρόνο τερματισμού λόγω αδράνειας της σύνδεσης. Τα 180 δευτερόλεπτα είναι η προεπιλεγμένη τιμή, έτσι η γραμμή αυτή είναι εδώ καθαρά διακοσμητική.

Γραμμή 9

Λέει στο PPP να ρωτήσει την άλλη πλευρά για να επιβεβαιώσει τις τοπικές ρυθμίσεις του resolver. Αν εκτελείτε τοπικό διακομιστή ονομάτων (DNS), θα πρέπει να μετατρέψετε αυτή τη γραμμή σε σχόλιο ή να την αφαιρέσετε.

Γραμμή 10

Κενή γραμμή ώστε η ανάγνωση του αρχείου να είναι πιο εύκολη. Οι κενές γραμμές αγνοούνται από το PPP.

Γραμμή 11

Αναγνωρίζει την καταχώριση ενός παροχέα με το όνομα "provider". Μπορείτε εδώ να χρησιμοποιήσετε το όνομα του ISP σας, ώστε αργότερα να ξεκινάτε τη σύνδεση σας με την επιλογή `load ISP`.

Γραμμή 12

Θέτει τον αριθμό κλήσης για αυτό τον παροχέα. Μπορείτε να καθορίσετε πολλαπλούς αριθμούς κλήσης χρησιμοποιώντας άνω-κάτω τελεία (`:`) ή τον χαρακτήρα (`|`) ως διαχωριστικό. Η διαφορά μεταξύ των δύο διαχωριστικών περιγράφεται στο ppp(8). Περιληπτικά, αν θέλετε να δοκιμάζονται κυκλικά όλοι οι αριθμοί, χρησιμοποιήστε την άνω-κάτω τελεία. Αν θέλετε να γίνεται πάντοτε απόπειρα κλήσης του πρώτου αριθμού και οι υπόλοιποι να δοκιμάζονται μόνο αν ο πρώτος αποτύχει, χρησιμοποιήστε το χαρακτήρα παροχέτευσης. Να γράφετε πάντοτε όλο το

σύνολο των τηλεφωνικών αριθμών με τον τρόπο που φαίνεται.

Αν ο αριθμός τηλεφώνου περιέχει κενά, θα πρέπει να τον περικλείσετε σε εισαγωγικά ("). Η παράλειψη τους, αν και είναι απλό σφάλμα, μπορεί να προκαλέσει προβλήματα που δεν μπορούν να εντοπιστούν εύκολα.

Γραμμές 13 & 14

Αναγνωρίζει το όνομα χρήστη και τον κωδικό του. Όταν συνδέεστε χρησιμοποιώντας προτροπή τύπου UNIX®, οι τιμές αυτές αναφέρονται από την εντολή `set login` χρησιμοποιώντας τις μεταβλητές \U και \P. Όταν συνδέεστε με χρήση PAP ή CHAP, οι τιμές αυτές χρησιμοποιούνται την ώρα της πιστοποίησης ταυτότητας του χρήστη.

Γραμμή 15

Αν χρησιμοποιείτε PPP ή CHAP, δεν θα υπάρχει στο σημείο αυτό προτροπή εισόδου (login), και θα πρέπει να μετατρέψετε τη γραμμή αυτή σε σχόλιο ή να την αφαιρέσετε. Δείτε την Πιστοποίηση PAP και CHAP για περισσότερες λεπτομέρειες.

Το αλφαριθμητικό εισόδου χρησιμοποιεί σύνταξη παρόμοια με το chat(8), όπως συμβαίνει και με το αλφαριθμητικό κλήσης. Στο παράδειγμα μας, το αλφαριθμητικό χρησιμοποιείται για μια υπηρεσία στην οποία η συνεδρία εισόδου μοιάζει με την παρακάτω:

```
J. Random Provider
login: foo
password: bar
protocol: ppp
```

Θα χρειαστεί να αλλάξετε αυτό το script ανάλογα με τις ανάγκες σας. Όταν γράφετε αυτό το script την πρώτη φορά, βεβαιωθείτε ότι έχετε ενεργοποιήσει το αρχείο καταγραφής για το "chat" ώστε να μπορείτε να προσδιορίσετε αν η διαδικασία αναγνώρισης προχωράει σωστά.

Γραμμή 16

Θέτει το χρόνο αδράνειας (σε δευτερόλεπτα) για τη σύνδεση. Εδώ, η σύνδεση θα κλείσει αυτόματα αν δεν υπάρχει κίνηση για 300 δευτερόλεπτα. Αν δεν θέλετε να γίνεται ποτέ τερματισμός της σύνδεσης λόγω αδράνειας, θέστε αυτή τη τιμή σε μηδέν, ή χρησιμοποιήστε την επιλογή `-ddial` στη γραμμή εντολής.

Γραμμή 17

Θέτει τη διεύθυνση της διεπαφής. Το αλφαριθμητικό *x.x.x.x* θα πρέπει να αντικατασταθεί με τη διεύθυνση IP που σας έχει αποδοθεί από τον παροχέα σας. Το αλφαριθμητικό *y.y.y.y* θα πρέπει να αντικατασταθεί με την διεύθυνση IP που έχει καθορίσει ο ISP σας ως πύλη (gateway, το μηχάνημα στο οποίο συνδέεστε). Αν ο ISP σας δεν σας έχει δώσει διεύθυνση πύλης, χρησιμοποιήστε την `10.0.0.2/0`. Αν πρέπει να χρησιμοποιήσετε μια IP διεύθυνση που έχετε "μαντέψει", βεβαιωθείτε ότι έχετε δημιουργήσει μια καταχώριση στο /etc/ppp/ppp.linkup σύμφωνα με τις οδηγίες για το PPP και Δυναμικές IP Διευθύνσεις. Αν παραλείψετε αυτή τη γραμμή, το `ppp` δεν θα μπορεί να εκτελεστεί σε κατάσταση `-auto`.

Γραμμή 18

Προσθέστε μια προεπιλεγμένη διαδρομή (default route) προς το μηχάνημα πύλης (gateway) του

ISP σας. Η ειδική λέξη HISADDR αντικαθίσταται με την διεύθυνση πύλης που καθορίζεται στη γραμμή 17. Είναι σημαντικό η γραμμή αυτή να εμφανίζεται μετά την γραμμή 17, διαφορετικά το HISADDR δεν θα έχει ακόμα λάβει αρχική τιμή.

Αν δεν επιθυμείτε να εκτελέσετε το ppp σε κατάσταση -auto, θα πρέπει να μετακινήσετε αυτή τη γραμμή στο αρχείο ppp.linkup.

Δεν είναι απαραίτητο να προσθέσετε καταχώριση στο αρχείο ppp.linkup όταν έχετε στατική διεύθυνση IP και εκτελείτε το ppp σε κατάσταση -auto. Στην περίπτωση αυτή, οι καταχωρίσεις σας στον πίνακα δρομολόγησης είναι σωστές πριν καν συνδεθείτε. Ίσως ωστόσο να θέλετε να δημιουργήσετε μια καταχώριση για να εκτελέσετε κάποια προγράμματα μετά την αποκατάσταση της σύνδεσης. Θα το εξηγήσουμε αυτό αργότερα σε ένα παράδειγμα με το sendmail.

Μπορείτε να βρείτε παραδείγματα αρχείων ρυθμίσεων στον κατάλογο usr/shared/examples/ppp/.

52.2.1.2.2. PPP και Δυναμικές Διευθύνσεις IP

Αν ο παροχέας σας δεν δίνει στατικές διευθύνσεις, το ppp μπορεί να ρυθμιστεί να διαπραγματεύεται την τοπική και την απομακρυσμένη διεύθυνση. Αυτό γίνεται "μαντεύοντας" μια διεύθυνση IP, και επιτρέποντας στο ppp να την θέσει έπειτα σωστά, χρησιμοποιώντας το πρωτόκολλο IPCP (IP Configuration Protocol) μετά τη σύνδεση. Το αρχείο ρυθμίσεων ppp.conf είναι το ίδιο όπως και στο PPP και Στατικές Διευθύνσεις IP, με την παρακάτω μόνο αλλαγή:

```
17      set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.255 0.0.0.0
```

Όπως και προηγουμένως, δεν πρέπει να περιλάβετε τον αριθμό γραμμής. Απαιτείται εσοχή ενός τουλάχιστον κενού διαστήματος.

Γραμμή 17

Ο αριθμός μετά το χαρακτήρα / είναι το πλήθος των bits της διεύθυνσης για το οποίο θα επιμείνει το ppp. Ίσως θέλετε να χρησιμοποιήσετε αριθμούς IP πιο κατάλληλους για την περίσταση, αλλά το παράδειγμα που δίνουμε παραπάνω θα λειτουργήσει πάντα.

Το τελευταίο όρισμα (το 0.0.0.0) λέει στο PPP να αρχίσει τις διαπραγματεύσεις με την διεύθυνση 0.0.0.0 αντί για την 10.0.0.1. Αυτό είναι απαραίτητο σε ορισμένους ISP. Μη χρησιμοποιήσετε το 0.0.0.0 ως πρώτο όρισμα στην set ifaddr, καθώς θα εμποδίσει την PPP να ρυθμίσει την αρχική διαδρομή στην κατάσταση -auto .

Αν δεν χρησιμοποιείτε την επιλογή -auto, θα χρειαστεί να δημιουργήσετε μια καταχώριση στο αρχείο /etc/ppp/ppp.linkup. Το αρχείο ppp.linkup χρησιμοποιείται μετά την αποκατάσταση της σύνδεσης. Στο σημείο αυτό, το ppp θα έχει ήδη αποδώσει διεύθυνση στην διεπαφή και θα είναι πλέον δυνατόν να προσθέσετε τις καταχωρίσεις στον πίνακα δρομολόγησης:

```
1     provider:
2      add default HISADDR
```

Γραμμή 1

Με την αποκατάσταση της σύνδεσης, το `ppp` θα ψάξει για μια καταχώριση στο ppp.linkup σύμφωνα με τους παρακάτω κανόνες: Αρχικά θα προσπαθήσει να ταιριάξει την πρώτη ετικέτα που έχει χρησιμοποιηθεί στο αρχείο ppp.conf. Αν αυτό αποτύχει, θα ψάξει για μια καταχώριση για την διεύθυνση IP της πύλης. Η καταχώριση αυτή είναι μια ετικέτα μορφής IP διεύθυνσης, με τέσσερις οκτάδες. Αν δεν έχει ακόμα βρεθεί η σωστή καταχώριση, θα γίνει ανίχνευση για την καταχώριση `MYADDR`.

Γραμμή 2

Η γραμμή αυτή λέει στο `ppp` να προσθέσει μια προεπιλεγμένη διαδρομή η οποία να δείχνει στο `HISADDR`. Το `HISADDR` θα αντικατασταθεί με τη διεύθυνση IP της πύλης όπως αυτή αποδόθηκε μέσω του πρωτοκόλλου IPCP.

Δείτε την καταχώριση `pmdemand` στα αρχεία /usr/shared/examples/ppp/ppp.conf.sample και /usr/shared/examples/ppp/ppp.linkup.sample για ένα πιο λεπτομερές παράδειγμα.

52.2.1.2.3. Λήψη Εισερχόμενων Κλήσεων

Όταν ρυθμίζετε το ppp να λαμβάνει εισερχόμενες κλήσεις σε ένα μηχάνημα που συνδέεται σε ένα τοπικό δίκτυο (LAN), θα πρέπει να αποφασίσετε αν θέλετε να προωθούνται πακέτα προς αυτό. Αν ναι, θα πρέπει να αποδώσετε στο μηχάνημα μια διεύθυνση IP η οποία να ανήκει στο ίδιο υποδίκτυο με το LAN, και να χρησιμοποιήσετε την εντολή `enable proxy` στο αρχείο /etc/ppp/ppp.conf. Θα πρέπει επίσης να επιβεβαιώσετε ότι το αρχείο /etc/rc.conf περιέχει τα παρακάτω:

```
gateway_enable="YES"
```

52.2.1.2.4. Ποιο getty;

Η ενότητα Υπηρεσία Εισόδου μέσω Επιλογικής Σύνδεσης (dial in) παρέχει μια καλή περιγραφή σχετικά με την ενεργοποίηση υπηρεσιών επιλογικών κλήσεων χρησιμοποιώντας την getty(8).

Μια εναλλακτική στην `getty` είναι η mgetty (από το πακέτο comms/mgetty+sendfax), μια πιο έξυπνη έκδοση της `getty`, η οποία έχει σχεδιαστεί για να λαμβάνει υπόψιν τις επιλογικές γραμμές.

Τα πλεονεκτήματα της `mgetty` είναι ότι *επικοινωνεί* ενεργά με τα modem, το οποίο σημαίνει ότι αν η θύρα είναι απενεργοποιημένη στο /etc/ttys, το modem σας δεν θα απαντήσει στην κλήση.

Μεταγενέστερες εκδόσεις της `mgetty` (από την 0.99beta και μετά) υποστηρίζουν επίσης αυτόματη ανίχνευση PPP streams, επιτρέποντας στους πελάτες σας πρόσβαση στον εξυπηρετητή χωρίς χρήση scripts.

Διαβάστε την ενότητα Mgetty και AutoPPP για περισσότερες πληροφορίες σχετικά με την `mgetty`.

52.2.1.2.5. Άδειες για το PPP

Φυσιολογικά, η εκτέλεση της εντολής `ppp` πρέπει να γίνεται ως χρήστης `root`. Αν ωστόσο θέλετε να επιτρέψετε την εκτέλεση του `ppp` σε κατάσταση εξυπηρετητή ως κανονικός χρήστης (με τον τρόπο που περιγράφεται παρακάτω) θα πρέπει να δώσετε σε αυτό το χρήστη τα κατάλληλα δικαιώματα για να εκτελεί το `ppp`, προσθέτοντας τον στην ομάδα `network` στο αρχείο /etc/group.

Θα πρέπει επίσης να τους δώσετε πρόσβαση σε ένα ή περισσότερα τμήματα του αρχείου ρυθμίσεων, χρησιμοποιώντας την εντολή `allow`:

```
allow users fred mary
```

Αν χρησιμοποιήσετε την επιλογή αυτή στο τμήμα `default`, θα δώσετε σε αυτούς τους χρήστες πρόσβαση σε όλες τις ρυθμίσεις.

52.2.1.2.6. Κελύφη PPP για Χρήστες με Δυναμικά IP

Δημιουργήστε ένα αρχείο με το όνομα /etc/ppp/ppp-shell το οποίο να περιέχει τα παρακάτω:

```
#!/bin/sh
IDENT=`echo $0 | sed -e 's/^.*-\(.*\)$/\1/'`
CALLEDAS="$IDENT"
TTY=`tty`

if [ x$IDENT = xdialup ]; then
        IDENT=`basename $TTY`
fi

echo "PPP for $CALLEDAS on $TTY"
echo "Starting PPP for $IDENT"

exec /usr/sbin/ppp -direct $IDENT
```

Το script αυτό θα πρέπει να γίνει εκτελέσιμο. Δημιουργήστε τώρα ένα συμβολικό δεσμό που να ονομάζεται ppp-dialup χρησιμοποιώντας τις παρακάτω εντολές:

```
# ln -s ppp-shell /etc/ppp/ppp-dialup
```

Θα πρέπει να χρησιμοποιήσετε αυτό το script ως το *κέλυφος* για όλους τους dialup χρήστες. Εδώ φαίνεται ένα παράδειγμα του /etc/passwd για ένα χρήστη dialup με όνομα `pchilds` (θυμηθείτε ότι δεν πρέπει να τροποποιείτε άμεσα το αρχείο των κωδικών, αλλά μέσω της εντολής vipw(8)).

```
pchilds:*:1011:300:Peter Childs PPP:/home/ppp:/etc/ppp/ppp-dialup
```

Δημιουργήστε ένα κατάλογο /home/ppp προσβάσιμο για ανάγνωση από όλους, ο οποίος θα περιέχει τα παρακάτω κενά αρχεία:

```
-r--r--r--   1 root     wheel           0 May 27 02:23 .hushlogin
-r--r--r--   1 root     wheel           0 May 27 02:22 .rhosts
```

τα οποία εμποδίζουν την εμφάνιση του μηνύματος από το αρχείο /etc/motd.

52.2.1.2.7. Κελύφη PPP για Χρήστες με Στατικό IP

Δημιουργήστε το αρχείο ppp-shell όπως φαίνεται παραπάνω, και για κάθε λογαριασμό με στατικό IP, δημιουργήστε ένα συμβολικό δεσμό προς το ppp-shell.

Για παράδειγμα, αν έχετε τρεις πελάτες dialup, τους `fred`, `sam`, και `mary`, στους οποίους εκτελείτε δρομολόγηση /24 CIDR, θα πρέπει να γράψετε τα παρακάτω:

```
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-fred
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-sam
# ln -s /etc/ppp/ppp-shell /etc/ppp/ppp-mary
```

Για κάθε λογαριασμό χρήστη dialup, θα πρέπει να ρυθμιστεί το κέλυφος στο συμβολικό δεσμό που δημιουργήθηκε παραπάνω (για παράδειγμα ο συμβολικός δεσμός για το κέλυφος του χρήστη `mary` θα πρέπει να είναι ο /etc/ppp/ppp-mary).

52.2.1.2.8. Ρύθμιση του ppp.conf για Χρήστες με Δυναμικό IP

Το αρχείο /etc/ppp/ppp.conf θα πρέπει να περιέχει κάτι αντίστοιχο με το παρακάτω:

```
default:
  set debug phase lcp chat
  set timeout 0

ttyu0:
  set ifaddr 203.14.100.1 203.14.100.20 255.255.255.255
  enable proxy

ttyu1:
  set ifaddr 203.14.100.1 203.14.100.21 255.255.255.255
  enable proxy
```

Η στοίχιση είναι σημαντική.

Για κάθε συνεδρία, φορτώνεται η ενότητα `default:`. Για κάθε γραμμή dialup που ενεργοποιείται στο /etc/ttys, θα πρέπει να δημιουργήσετε μια καταχώριση όμοια με αυτή που φαίνεται παραπάνω για το `ttyu0:`. Κάθε γραμμή θα πρέπει να παίρνει μια μοναδική διεύθυνση IP από το απόθεμα των IP διευθύνσεων που προορίζονται για τους δυναμικούς χρήστες.

52.2.1.2.9. Ρύθμιση του ppp.conf για Χρήστες με Στατικό IP

Εκτός από τα περιεχόμενα του υποδείγματος /usr/shared/examples/ppp/ppp.conf θα πρέπει να προσθέσετε μια ενότητα για καθένα από τους χρήστες dialup στους οποίους έχει αποδοθεί στατικό IP. Θα συνεχίσουμε με το παράδειγμα μας με τους χρήστες `fred`, `sam`, και `mary`.

```
fred:
  set ifaddr 203.14.100.1 203.14.101.1 255.255.255.255
```

```
sam:
  set ifaddr 203.14.100.1 203.14.102.1 255.255.255.255

mary:
  set ifaddr 203.14.100.1 203.14.103.1 255.255.255.255
```

Το αρχείο /etc/ppp/ppp.linkup θα πρέπει επίσης να περιέχει πληροφορίες δρομολόγησης για κάθε χρήστη με στατικό IP (αν απαιτείται). Η παρακάτω γραμμή θα προσθέσει μια διαδρομή προς τη διεύθυνση δικτύου 203.14.101.0/24 μέσω της σύνδεσης ppp του πελάτη.

```
fred:
  add 203.14.101.0 netmask 255.255.255.0 HISADDR

sam:
  add 203.14.102.0 netmask 255.255.255.0 HISADDR

mary:
  add 203.14.103.0 netmask 255.255.255.0 HISADDR
```

52.2.1.2.10. mgetty και AutoPPP

Το port comms/mgetty+sendfax, έρχεται με προεπιλεγμένη την επιλογή AUTO_PPP, επιτρέποντας έτσι στην mgetty να ανιχνεύει την φάση LCP των συνδέσεων PPP και να εκτελεί αυτόματα ένα κέλυφος ppp. Ωστόσο, καθώς με αυτό τον τρόπο δεν ενεργοποιείται η προεπιλεγμένη ακολουθία ονόματος χρήστη και κωδικού, είναι απαραίτητο να γίνει πιστοποίηση των χρηστών με τη χρήση PAP ή CHAP.

Η ενότητα αυτή προϋποθέτει ότι ο χρήστης έχει ρυθμίσει, μεταγλωττίσει και εγκαταστήσει με επιτυχία το port comms/mgetty+sendfax στο σύστημα του.

Βεβαιωθείτε ότι το αρχείο σας /usr/local/etc/mgetty+sendfax/login.config περιέχει τα παρακάτω:

```
/AutoPPP/ -     -            /etc/ppp/ppp-pap-dialup
```

Αυτό θα πει στην mgetty να εκτελέσει το script ppp-pap-dialup για τις PPP συνδέσεις που ανιχνεύθηκαν.

Δημιουργήστε ένα αρχείο με το όνομα /etc/ppp/ppp-pap-dialup το οποίο θα περιέχει τα ακόλουθα (το αρχείο θα πρέπει να είναι εκτελέσιμο):

```
#!/bin/sh
exec /usr/sbin/ppp -direct pap$IDENT
```

Για κάθε γραμμή dialup που είναι ενεργοποιημένη στο /etc/ttys, δημιουργήστε μια αντίστοιχη καταχώριση στο αρχείο /etc/ppp/ppp.conf. Η καταχώριση αυτή μπορεί να συνυπάρχει χωρίς πρόβλημα με αυτές που ορίσαμε παραπάνω.

```
pap:
  enable pap
  set ifaddr 203.14.100.1 203.14.100.20-203.14.100.40
  enable proxy
```

Κάθε χρήστης που εισέρχεται με αυτό τον τρόπο, θα πρέπει να διαθέτει όνομα χρήστη/κωδικό στο αρχείο /etc/ppp/ppp.secret. Εναλλακτικά, μπορείτε να προσθέσετε την παρακάτω επιλογή ώστε να γίνεται πιστοποίηση των χρηστών μέσω PAP με βάση τα στοιχεία του αρχείου /etc/passwd.

```
enable passwdauth
```

Αν θέλετε να αποδώσετε στατικό IP σε κάποιους χρήστες, μπορείτε να καθορίσετε την διεύθυνση ως τρίτο όρισμα στο αρχείο /etc/ppp/ppp.secret. Για παραδείγματα, δείτε το αρχείο /usr/shared/examples/ppp/ppp.secret.sample.

52.2.1.2.11. Επεκτάσεις MS

Είναι δυνατόν να ρυθμίσετε το PPP ώστε να παρέχει διευθύνσεις DNS και NetBIOS κατά απαίτηση.

Για να ενεργοποιήσετε αυτές τις επεκτάσεις με την έκδοση 1.x του PPP, θα πρέπει να προσθέσετε τις παρακάτω γραμμές στο σχετικό τμήμα του /etc/ppp/ppp.conf.

```
enable msext
set ns 203.14.100.1 203.14.100.2
set nbns 203.14.100.5
```

Για το PPP από την έκδοση 2 και πάνω:

```
accept dns
set dns 203.14.100.1 203.14.100.2
set nbns 203.14.100.5
```

Το παραπάνω θα ενημερώσει τους πελάτες για τον κύριο και δευτερεύοντα εξυπηρετητή DNS, και για τον εξυπηρετητή ονομάτων NetBIOS.

Από την έκδοση 2 και πάνω, αν παραλειφθεί η γραμμή `set dns`, το PPP θα χρησιμοποιήσει τις γραμμές που θα βρει στο /etc/resolv.conf.

52.2.1.2.12. Πιστοποίηση PAP και CHAP

Κάποιοι ISP ρυθμίζουν τα συστήματα τους με τέτοιο τρόπο, ώστε το κομμάτι της σύνδεσης που ασχολείται με την πιστοποίηση του χρήστη να γίνεται μέσω των μηχανισμών PAP ή CHAP. Αν συμβαίνει αυτό στη δική σας περίπτωση, ο ISP σας δεν θα σας στείλει προτροπή login όταν συνδεθείτε, αλλά θα αρχίσει απευθείας τη μετάδοση PPP.

Το PAP είναι λιγότερο ασφαλές από το CHAP, αλλά η ασφάλεια εδώ δεν είναι τόσο σπουδαίο θέμα,

καθώς οι κωδικοί (αν και στέλνονται ως κανονικό κείμενο) μεταδίδονται μόνο μέσω σειριακής γραμμής. Έτσι δεν υπάρχει πραγματική δυνατότητα των crackers να "κρυφακούσουν".

Χρησιμοποιώντας ως αναφορά τις ενότητες PPP και Στατικές Διευθύνσεις IP ή PPP και Δυναμικές Διευθύνσεις IP, θα πρέπει να γίνουν οι παρακάτω αλλαγές:

```
13      set authname MyUserName
14      set authkey MyPassword
15      set login
```

Γραμμή 13

Η γραμμή αυτή καθορίζει το όνομα χρήστη για τα PAP/CHAP. Θα χρειαστεί να εισάγετε την σωστή τιμή για το *MyUserName*.

Γραμμή 14

Η γραμμή αυτή καθορίζει τον κωδικό για τα PAP/CHAP. Θα χρειαστεί να εισάγετε την σωστή τιμή για το *MyPassword*. Ίσως θέλετε να προσθέσετε μια ακόμα γραμμή, όπως την παρακάτω:

```
16      accept PAP
```

ή

```
16      accept CHAP
```

για να είναι φανερή η πρόθεση σας, ωστόσο τόσο το PAP όσο και το CHAP γίνονται δεκτά από προεπιλογή.

Γραμμή 15

Ο ISP σας δεν θα απαιτεί φυσιολογικά να εισέλθετε στον εξυπηρετητή αν χρησιμοποιείτε PAP ή CHAP. Για το λόγο αυτό, θα πρέπει να απενεργοποιήσετε το αλφαριθμητικό "set login".

52.2.1.2.13. Αλλάζοντας Άμεσα τις Ρυθμίσεις του `ppp`

Είναι δυνατόν να επικοινωνήσετε με το πρόγραμμα `ppp` καθώς εκτελείται στον παρασκήνιο, αλλά μόνο αν έχετε ρυθμίσει μια κατάλληλη διαγνωστική θύρα για αυτό το σκοπό. Για να το κάνετε αυτό, προσθέστε την παρακάτω γραμμή στις ρυθμίσεις σας:

```
set server /var/run/ppp-tun%d DiagnosticPassword 0177
```

Αυτό οδηγεί το PPP να "ακούει" στο καθορισμένο UNIX® socket του τομέα, και να ρωτάει τους πελάτες για τον κωδικό που έχει καθοριστεί πριν επιτρέψει την πρόσβαση. Το `%d` στο όνομα, αντικαθίσταται με τον αριθμό της συσκευής tun που χρησιμοποιείται.

Από τη στιγμή που ρυθμιστεί το socket, το πρόγραμμα pppctl(8) μπορεί να χρησιμοποιηθεί σε scripts με τα οποία επιθυμείτε να διαχειριστείτε το πρόγραμμα `ppp` το οποίο εκτελείται ήδη.

52.2.1.3. Χρησιμοποιώντας τη Δυνατότητα Μετάφρασης Διευθύνσεων (NAT) του PPP

Το PPP έχει την ικανότητα να χρησιμοποιήσει δικό του εσωτερικό NAT, χωρίς να απαιτούνται οι ικανότητες ανακατεύθυνσης του πυρήνα. Μπορείτε να ενεργοποιήσετε αυτή τη λειτουργία με την ακόλουθη γραμμή στο /etc/ppp/ppp.conf:

```
nat enable yes
```

Εναλλακτικά, το NAT του PPP μπορεί να ενεργοποιηθεί με την επιλογή `-nat` στην γραμμή εντολών. Μπορείτε ακόμα να βάλετε την επιλογή `ppp_nat` στο αρχείο /etc/rc.conf. Η επιλογή αυτή είναι ενεργοποιημένη από προεπιλογή.

Αν χρησιμοποιήσετε αυτό το χαρακτηριστικό, μάλλον θα βρείτε χρήσιμες και τις παρακάτω επιλογές για το /etc/ppp/ppp.conf, με τις οποίες ενεργοποιείται η προώθηση εισερχόμενων συνδέσεων:

```
nat port tcp 10.0.0.2:ftp ftp
nat port tcp 10.0.0.2:http http
```

ή αν δεν εμπιστεύεστε καθόλου το εξωτερικό δίκτυο:

```
nat deny_incoming yes
```

52.2.1.4. Τελικές Ρυθμίσεις Συστήματος

Έχετε πλέον ρυθμίσει το `ppp`, αλλά υπάρχουν μερικά ακόμα πράγματα που πρέπει να κάνετε πριν να είναι έτοιμο για λειτουργία. Όλα περιλαμβάνουν την επεξεργασία του αρχείου /etc/rc.conf.

Ξεκινώντας από την αρχή του αρχείου αυτού, βεβαιωθείτε ότι είναι ορισμένη η γραμμή `hostname=`, π.χ.:

```
hostname="foo.example.com"
```

Αν ο ISP σας παρέχει στατική IP διεύθυνση και όνομα, είναι μάλλον καλύτερο να χρησιμοποιήσετε αυτό το όνομα ως όνομα για το μηχάνημα σας.

Ψάξτε για τη μεταβλητή `network_interfaces`. Αν θέλετε να ρυθμίσετε το σύστημα σας να καλεί τον ISP σας κατά απαίτηση, βεβαιωθείτε ότι υπάρχει στη λίστα η συσκευή tun0, διαφορετικά αφαιρέστε την.

```
network_interfaces="lo0 tun0"
ifconfig_tun0=
```

Η μεταβλητή `ifconfig_tun0` θα πρέπει να είναι άδεια, και θα πρέπει να δημιουργηθεί ένα αρχείο με όνομα /etc/start_if.tun0. Το αρχείο αυτό θα πρέπει να

περιέχει την παρακάτω γραμμή:

```
ppp -auto mysystem
```

Το script αυτό εκτελείται κατά τη διάρκεια ρύθμισης του δικτύου, ξεκινώντας έτσι το δαίμονα ppp σε κατάσταση αυτόματης λειτουργίας. Αν διαθέτετε κάποιο τοπικό δίκτυο (LAN) για το οποίο το μηχάνημα αυτό έχει το ρόλο της πύλης, ίσως να θέλετε επίσης να χρησιμοποιήσετε την επιλογή `-alias`. Δείτε τη σελίδα manual για περισσότερες λεπτομέρειες.

Βεβαιωθείτε ότι η μεταβλητή για το πρόγραμμα router έχει τεθεί στο `NO` μέσω της επόμενης γραμμής στο /etc/rc.conf:

```
router_enable="NO"
```

Είναι σημαντικό να μην ξεκινήσει ο δαίμονας `routed`, ο οποίος συνήθως διαγράφει τις προεπιλεγμένες τιμές του πίνακα δρομολόγησης που δημιουργούνται από το `ppp`.

Είναι μάλλον καλή ιδέα να εξασφαλίσετε ότι η γραμμή `sendmail_flags` δεν περιλαμβάνει την επιλογή `-q`, διαφορετικά το `sendmail` θα προσπαθεί κάθε τόσο να κάνει αναζήτηση του δικτύου, με πιθανό αποτέλεσμα το μηχάνημα σας να εκτελεί τηλεφωνική σύνδεση (dial out). Μπορείτε να δοκιμάσετε:

```
sendmail_flags="-bd"
```

Το μειονέκτημα του παραπάνω, είναι ότι πρέπει να εξαναγκάσετε το `sendmail` να επανεξετάσει την ουρά των μηνυμάτων, κάθε φορά που αποκαθίσταται η σύνδεση ppp, γράφοντας:

```
# /usr/sbin/sendmail -q
```

Ίσως θέλετε να χρησιμοποιήσετε την εντολή `!bg` στο ppp.linkup για να γίνεται το παραπάνω αυτόματα:

```
1     provider:
2       delete ALL
3       add 0 0 HISADDR
4       !bg sendmail -bd -q30m
```

Αν αυτό δεν σας αρέσει, είναι δυνατόν να ρυθμίσετε ένα "dfilter" το οποίο να αποκόπτει την κίνηση SMTP. Δείτε τα υποδείγματα για περισσότερες λεπτομέρειες.

Το μόνο που μένει είναι να επανεκκινήσετε το μηχάνημα. Μετά την επανεκκίνηση, μπορείτε είτε να γράψετε:

```
# ppp
```

και έπειτα `dial provider` για να ξεκινήσετε τη συνεδρία PPP, ή αν θέλετε το `ppp` να αποκαθιστά τις συνεδρίες αυτόματα κάθε φορά που υπάρχει κίνηση προς το εξωτερικό δίκτυο (και δεν έχετε δημιουργήσει το script start_if.tun0) μπορείτε να γράψετε:

```
# ppp -auto provider
```

52.2.1.5. Περίληψη

Για να ανακεφαλαιώσουμε, τα παρακάτω βήματα είναι απαραίτητα όταν εγκαθιστάτε το ppp για πρώτη φορά:

Από τη μεριά του μηχανήματος-πελάτη:

1. Βεβαιωθείτε ότι περιλαμβάνεται στον πυρήνα σας η συσκευή tun.
2. Βεβαιωθείτε ότι υπάρχει το αρχείο της συσκευής tunN στον κατάλογο /dev.
3. Δημιουργήστε μια καταχώριση στο αρχείο /etc/ppp/ppp.conf. Το παράδειγμα για το pmdemand θα πρέπει να είναι επαρκές για τους περισσότερους ISPs.
4. Αν έχετε δυναμική διεύθυνση IP, δημιουργήστε μια καταχώριση στο /etc/ppp/ppp.linkup.
5. Ενημερώστε το αρχείο /etc/rc.conf.
6. Δημιουργήστε το script start_if.tun0 αν χρειάζεστε κλήση κατά απαίτηση.

Από τη μεριά του εξυπηρετητή:

1. Βεβαιωθείτε ότι περιλαμβάνεται στον πυρήνα σας η συσκευή tun.
2. Βεβαιωθείτε ότι υπάρχει το αρχείο της συσκευής tunN στον κατάλογο /dev.
3. Δημιουργήστε μια καταχώριση στο /etc/passwd (χρησιμοποιώντας το πρόγραμμα vipw(8)).
4. Δημιουργήστε ένα αρχείο profile στον προσωπικό κατάλογο του χρήστη, το οποίο να εκτελεί την εντολή `ppp -direct direct-server` ή κάποια αντίστοιχη.
5. Δημιουργήστε μια καταχώριση στο /etc/ppp/ppp.conf. Το παράδειγμα για το direct-server θα πρέπει να είναι επαρκές.
6. Δημιουργήστε μια καταχώριση στο /etc/ppp/ppp.linkup.
7. Ενημερώστε το αρχείο /etc/rc.conf.

52.3. Χρησιμοποιώντας το PPP του Πυρήνα

Η ενότητα αυτή είναι έγκυρη και μπορεί να εφαρμοστεί μόνο σε συστήματα FreeBSD 7.X.

52.3.1. Ρυθμίζοντας το PPP του Πυρήνα

Πριν ξεκινήσετε να ρυθμίζετε το PPP στο μηχάνημα σας, βεβαιωθείτε ότι το pppd βρίσκεται στον κατάλογο /usr/sbin και ότι υπάρχει ο κατάλογος /etc/ppp.

Το pppd έχει δύο καταστάσεις λειτουργίας:

1. Ως πελάτης ("client") - όταν θέλετε να συνδέσετε το μηχάνημα σας με τον έξω κόσμο μέσω σειριακής σύνδεσης σύνδεσης ή γραμμής modem.
2. Ως εξυπηρετητής ("server") - το μηχάνημα σας είναι συνδεμένο στο δίκτυο και χρησιμοποιείται για να συνδέσει άλλους υπολογιστές, χρησιμοποιώντας το PPP.

Και στις δύο περιπτώσεις θα χρειαστεί να δημιουργήσετε ένα αρχείο επιλογών (/etc/ppp/options ή ~/.ppprc αν στο μηχάνημα σας υπάρχουν περισσότεροι από ένας χρήστες που χρησιμοποιούν το PPP).

Θα χρειαστείτε επίσης και κάποιο λογισμικό για χρήση με modem και σειριακές συνδέσεις (κατά προτίμηση το comms/kermit), ώστε να μπορείτε να καλέσετε και να αποκαταστήσετε τη σύνδεση με τον απομακρυσμένο εξυπηρετητή.

52.3.2. Χρησιμοποιώντας το pppd ως Πελάτης

Μπορείτε να χρησιμοποιήσετε το /etc/ppp/options που φαίνεται παρακάτω, για να συνδεθείτε σε μια γραμμή PPP ενός εξυπηρετητή τερματικών (terminal server) της Cisco.

```
crtscts         # enable hardware flow control
modem           # modem control line
noipdefault     # remote PPP server must supply your IP address
                # if the remote host does not send your IP during IPCP
                # negotiation, remove this option
passive         # wait for LCP packets
domain ppp.foo.com      # put your domain name here

:remote_ip    # put the IP of remote PPP host here
                # it will be used to route packets via PPP link
                # if you didn't specified the noipdefault option
                # change this line to local_ip:remote_ip

defaultroute    # put this if you want that PPP server will be your
                # default router
```

Για να συνδεθείτε:

1. Καλέστε τον απομακρυσμένο εξυπηρετητή χρησιμοποιώντας το Kermit (ή κάποιο άλλο πρόγραμμα για modem) και εισάγετε το όνομα χρήστη και τον κωδικό σας (ή ότι άλλο χρειάζεται για να ενεργοποιήσετε το PPP στον απομακρυσμένο υπολογιστή).
2. Βγείτε από το Kermit (χωρίς να κλείσετε τη γραμμή).
3. Πληκτρολογήστε τα παρακάτω:

```
# /usr/sbin/pppd /dev/tty01 19200
```

Βεβαιωθείτε ότι χρησιμοποιείτε το σωστό όνομα συσκευής και την κατάλληλη ταχύτητα.

Ο υπολογιστής σας είναι τώρα συνδεμένος μέσω PPP. Αν η σύνδεση αποτύχει, μπορείτε να χρησιμοποιήσετε την επιλογή `debug` στο αρχείο /etc/ppp/options και να ελέγξετε τα μηνύματα στην κονσόλα για να ανιχνεύσετε το πρόβλημα.

Το παρακάτω script /etc/ppp/pppup αυτοματοποιεί και τα 3 στάδια:

```
#!/bin/sh
pgrep -l pppd
pid=`pgrep pppd`
if [ "X${pid}" != "X" ] ; then
        echo 'killing pppd, PID=' ${pid}
        kill ${pid}
fi
pgrep -l kermit
pid=`pgrep kermit`
if [ "X${pid}" != "X" ] ; then
        echo 'killing kermit, PID=' ${pid}
        kill -9 ${pid}
fi

ifconfig ppp0 down
ifconfig ppp0 delete

kermit -y /etc/ppp/kermit.dial
pppd /dev/tty01 19200
```

Το αρχείο /etc/ppp/kermit.dial είναι ένα script για το Kermit το οποίο κάνει την κλήση και την πιστοποίηση του χρήστη στον απομακρυσμένο υπολογιστή (στο τέλος αυτού του εγγράφου, θα βρείτε ένα παράδειγμα για ένα τέτοιο script).

Χρησιμοποιήστε το παρακάτω script /etc/ppp/pppdown για να αποσυνδέσετε την γραμμή PPP:

```
#!/bin/sh
pid=`pgrep pppd`
if [ X${pid} != "X" ] ; then
        echo 'killing pppd, PID=' ${pid}
        kill -TERM ${pid}
fi

pgrep -l kermit
pid=`pgrep kermit`
if [ "X${pid}" != "X" ] ; then
        echo 'killing kermit, PID=' ${pid}
        kill -9 ${pid}
```

```
fi

/sbin/ifconfig ppp0 down
/sbin/ifconfig ppp0 delete
kermit -y /etc/ppp/kermit.hup
/etc/ppp/ppptest
```

Ελέγξτε αν εκτελείται ακόμα το pppd, εκτελώντας το /usr/etc/ppp/ppptest, το οποίο θα μοιάζει με το παρακάτω:

```
#!/bin/sh
pid=`pgrep pppd`
if [ X${pid} != "X" ] ; then
        echo 'pppd running: PID=' ${pid-NONE}
else
        echo 'No pppd running.'
fi
set -x
netstat -n -I ppp0
ifconfig ppp0
```

Για να κλείσετε την γραμμή, εκτελέστε το /etc/ppp/kermit.hup, το οποίο θα πρέπει να περιέχει:

```
set line /dev/tty01 ; put your modem device here
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++
inp 5 OK
out ATH0\13
echo \13
exit
```

Μια εναλλακτική μέθοδος που χρησιμοποιεί το chat αντί για το kermit:

Τα παρακάτω δύο αρχεία επαρκούν για τη δημιουργία μιας σύνδεσης pppd.

/etc/ppp/options:

```
/dev/cuad1 115200

crtscts     # enable hardware flow control
modem       # modem control line
connect "/usr/bin/chat -f /etc/ppp/login.chat.script"
noipdefault # remote PPP serve must supply your IP address
            # if the remote host doesn't send your IP during
                # IPCP negotiation, remove this option
passive         # wait for LCP packets
domain your.domain  # put your domain name here

:       # put the IP of remote PPP host here
            # it will be used to route packets via PPP link
                # if you didn't specified the noipdefault option
                # change this line to local_ip:remote_ip

defaultroute    # put this if you want that PPP server will be
            # your default router
```

/etc/ppp/login.chat.script:

Το παρακάτω θα πρέπει να γραφεί σε μια μόνο γραμμή.

```
ABORT BUSY ABORT 'NO CARRIER' "" AT OK ATDTphone.number
  CONNECT "" TIMEOUT 10 ogin:-\\r-ogin: login-id
  TIMEOUT 5 sword: password
```

Μόλις τροποποιήσετε και εγκαταστήσετε σωστά τα παραπάνω αρχεία, το μόνο που χρειάζεται να κάνετε είναι να εκτελέσετε την εντολή pppd, με τον τρόπο που φαίνεται παρακάτω:

```
# pppd
```

52.3.3. Χρησιμοποιώντας το pppd ως Εξυπηρετητή

Το /etc/ppp/options θα πρέπει να περιέχει κάτι αντίστοιχο με το παρακάτω:

```
crtscts                         # Hardware flow control
netmask 255.255.255.0           # netmask (not required)
192.114.208.20:192.114.208.165  # IP's of local and remote hosts
                                # local ip must be different from one
                                # you assigned to the Ethernet (or other)
                                # interface on your machine.
                                # remote IP is IP address that will be
                                # assigned to the remote machine
domain ppp.foo.com              # your domain
passive                         # wait for LCP
```

```
modem                           # modem line
```

Το script /etc/ppp/pppserv που φαίνεται παρακάτω, θα πει στο pppd να λειτουργήσει ως εξυπηρετητής:

```
#!/bin/sh
pgrep -l pppd
pid=`pgrep pppd`
if [ "X${pid}" != "X" ] ; then
        echo 'killing pppd, PID=' ${pid}
        kill ${pid}
fi
pgrep -l kermit
pid=`pgrep kermit`
if [ "X${pid}" != "X" ] ; then
        echo 'killing kermit, PID=' ${pid}
        kill -9 ${pid}
fi

# reset ppp interface
ifconfig ppp0 down
ifconfig ppp0 delete

# enable autoanswer mode
kermit -y /etc/ppp/kermit.ans

# run ppp
pppd /dev/tty01 19200
```

Χρησιμοποιήστε το παρακάτω script /etc/ppp/pppservdown για να σταματήσετε τον εξυπηρετητή:

```
#!/bin/sh
pgrep -l pppd
pid=`pgrep pppd`
if [ "X${pid}" != "X" ] ; then
        echo 'killing pppd, PID=' ${pid}
        kill ${pid}
fi
pgrep -l kermit
pid=`pgrep kermit`
if [ "X${pid}" != "X" ] ; then
        echo 'killing kermit, PID=' ${pid}
        kill -9 ${pid}
fi
ifconfig ppp0 down
ifconfig ppp0 delete

kermit -y /etc/ppp/kermit.noans
```

Το παρακάτω script για το Kermit (/etc/ppp/kermit.ans) μπορεί να ενεργοποιεί και να απενεργοποιεί την λειτουργία αυτόματης απάντησης στο modem σας.

```
set line /dev/tty01
set speed 19200
set file type binary
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
set flow none

pau 1
out +++
inp 5 OK
out ATH0\13
inp 5 OK
echo \13
out ATS0=1\13   ; change this to out ATS0=0\13 if you want to disable
                ; autoanswer mode
inp 5 OK
echo \13
exit
```

Στον απομακρυσμένο υπολογιστή, χρησιμοποιείται το script /etc/ppp/kermit.dial για κλήση και πιστοποίηση του χρήστη. Θα πρέπει να το τροποποιήσετε σύμφωνα με τις ανάγκες σας. Βάλτε το όνομα χρήστη και τον κωδικό σας σε αυτό το script. Θα χρειαστεί επίσης να αλλάξετε την γραμμή για την είσοδο (input) ανάλογα με τις απαντήσεις που δίνει το modem σας και ο απομακρυσμένος υπολογιστής.

```
;
; put the com line attached to the modem here:
;
set line /dev/tty01
;
; put the modem speed here:
;
set speed 19200
set file type binary            ; full 8 bit file xfer
set file names literal
set win 8
set rec pack 1024
set send pack 1024
set block 3
set term bytesize 8
set command bytesize 8
```

```
set flow none
set modem hayes
set dial hangup off
set carrier auto                ; Then SET CARRIER if necessary,
set dial display on             ; Then SET DIAL if necessary,
set input echo on
set input timeout proceed
set input case ignore
def \%x 0                       ; login prompt counter
goto slhup

:slcmd                          ; put the modem in command mode
echo Put the modem in command mode.
clear                           ; Clear unread characters from input buffer
pause 1
output +++                      ; hayes escape sequence
input 1 OK\13\10                ; wait for OK
if success goto slhup
output \13
pause 1
output at\13
input 1 OK\13\10
if fail goto slcmd              ; if modem doesn't answer OK, try again

:slhup                          ; hang up the phone
clear                           ; Clear unread characters from input buffer
pause 1
echo Hanging up the phone.
output ath0\13                  ; hayes command for on hook
input 2 OK\13\10
if fail goto slcmd              ; if no OK answer, put modem in command mode

:sldial                         ; dial the number
pause 1
echo Dialing.
output atdt9,550311\13\10               ; put phone number here
assign \%x 0                    ; zero the time counter

:look
clear                           ; Clear unread characters from input buffer
increment \%x                   ; Count the seconds
input 1 {CONNECT }
if success goto sllogin
reinput 1 {NO CARRIER\13\10}
if success goto sldial
reinput 1 {NO DIALTONE\13\10}
if success goto slnodial
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
```

```
if < \%x 60 goto look
else goto slhup

:sllogin                        ; login
assign \%x 0                    ; zero the time counter
pause 1
echo Looking for login prompt.

:slloop
increment \%x                   ; Count the seconds
clear                           ; Clear unread characters from input buffer
output \13
;
; put your expected login prompt here:
;
input 1 {Username: }
if success goto sluid
reinput 1 {\255}
if success goto slhup
reinput 1 {\127}
if success goto slhup
if < \%x 10 goto slloop         ; try 10 times to get a login prompt
else goto slhup                 ; hang up and start again if 10 failures

:sluid
;
; put your userid here:
;
output ppp-login\13
input 1 {Password: }
;
; put your password here:
;
output ppp-password\13
input 1 {Entering SLIP mode.}
echo
quit

:slnodial
echo \7No dialtone.  Check the telephone line!\7
exit 1

; local variables:
; mode: csh
; comment-start: "; "
; comment-start-skip: "; "
; end:
```

52.4. Αντιμετώπιση Προβλημάτων σε Συνδέσεις PPP

Από το FreeBSD 8.0 και μετά, το πρόγραμμα οδήγησης sio(4) αντικαταστάθηκε από το uart(4). Τα ονόματα συσκευών των σειριακών θυρών έχουν αλλάξει από /dev/cuadN σε /dev/cuauN και από /dev/ttydN σε /dev/ttyuN. Οι χρήστες του FreeBSD 7.X θα πρέπει να προσαρμόσουν τις παρακάτω οδηγίες σύμφωνα με αυτές τις αλλαγές.

Η ενότητα αυτή καλύπτει μερικά από τα προβλήματα που μπορεί να παρουσιαστούν όταν γίνεται χρήση του PPP μέσω σύνδεσης modem. Για παράδειγμα, θα πρέπει να ξέρετε με ακρίβεια τα μηνύματα εισόδου που θα εμφανίσει το σύστημα το οποίο καλείτε. Μερικοί ISP δίνουν την προτροπή `ssword`, ενώ άλλοι δίνουν την `password`. Αν δεν έχετε γράψει σωστά το script για το `ppp`, η απόπειρα εισόδου θα αποτύχει. Ο πιο συνηθισμένος τρόπος να εκσφαλματώσετε μια σύνδεση `ppp`, είναι να συνδεθείτε χειροκίνητα. Οι πληροφορίες που εμφανίζονται παρακάτω, θα σας οδηγήσουν βήμα προς βήμα στη χειροκίνητη αποκατάσταση της σύνδεσης.

52.4.1. Ελέγξτε τα Αρχεία Συσκευών

Αν χρησιμοποιείτε προσαρμοσμένο πυρήνα, βεβαιωθείτε ότι έχετε περιλάβει την παρακάτω γραμμή στο αρχείο ρυθμίσεων του πυρήνα σας:

```
device   uart
```

Αν χρησιμοποιείτε τον πυρήνα `GENERIC`, δεν χρειάζεται να κάνετε κάποια αλλαγή, καθώς η συσκεύη uart περιλαμβάνεται ήδη σε αυτόν. Απλώς ελέγξτε τα μηνύματα της `dmesg` για την συσκευή modem, χρησιμοποιώντας την παρακάτω εντολή:

```
# dmesg | grep uart
```

Θα πρέπει να δείτε κάποια έξοδο σχετική με τις συσκευές uart. Πρόκειται για τις θύρες COM που χρειαζόμαστε. Αν το modem σας λειτουργεί ως τυποποιημένη σειριακή θύρα, θα πρέπει να το δείτε να αναφέρεται ως uart1, ή COM2. Αν συμβαίνει αυτό, δεν χρειάζεται να επαναμεταγλωττίσετε τον πυρήνα σας. Αν η σειριακή θύρα που αντιστοιχεί στο modem σας είναι η uart1 ή COM2 στο DOS, η αντίστοιχη συσκευή modem θα είναι η /dev/cuau1.

52.4.2. Χειροκίνητη Σύνδεση

Η χειροκίνητη σύνδεση στο Internet με χρήση της `ppp`, είναι ένας γρήγορος και εύκολος τρόπος να εντοπίσετε τυχόν προβλήματα σύνδεσης, ή απλώς να πάρετε πληροφορίες σχετικά με το πως ο ISP σας αντιμετωπίζει τις συνδέσεις πελατών `ppp`. Θα ξεκινήσουμε την εφαρμογή PPP από την γραμμή εντολών. Σημειώστε ότι σε όλα μας τα παραδείγματα, θα χρησιμοποιούμε το *example* ως το όνομα του υπολογιστή που εκτελεί το PPP. Μπορείτε να ξεκινήσετε το `ppp`, γράφοντας απλώς `ppp`:

```
# ppp
```

Έχουμε τώρα ξεκινήσει το ppp.

```
ppp ON example> set device /dev/cuau1
```

Θέτουμε τη συσκευή modem. Στο παράδειγμα μας, είναι η cuau1.

```
ppp ON example> set speed 115200
```

Θέτουμε την ταχύτητα σύνδεσης, σε αυτή την περίπτωση χρησιμοποιούμε 115,200 kbps.

```
ppp ON example> enable dns
```

Λέμε στο ppp να ρυθμίσει τον resolver και προσθέτουμε τις κατάλληλες γραμμές για το διακομιστή ονομάτων στο /etc/resolv.conf. Αν το ppp δεν μπορεί να καθορίσει το όνομα του διακομιστή, μπορούμε να το καθορίσουμε με χειροκίνητο τρόπο αργότερα.

```
ppp ON example> term
```

Αλλάζουμε σε κατάσταση "terminal" ώστε να μπορούμε να ελέγξουμε το modem χειροκίνητα.

```
deflink: Entering terminal mode on /dev/cuau1
type '~h' for help
```

```
at
OK
atdt123456789
```

Χρησιμοποιούμε το at για να αρχικοποιήσουμε το modem, και έπειτα χρησιμοποιούμε το atdt και τον αριθμό του ISP για να ξεκινήσουμε τη διαδικασία της κλήσης.

```
CONNECT
```

Εδώ έχουμε επιβεβαίωση της σύνδεσης. Αν έχουμε προβλήματα σύνδεσης τα οποία δεν σχετίζονται με το υλικό μας, εδώ είναι το σημείο που πρέπει να προσπαθήσουμε να τα επιλύσουμε.

```
ISP Login:myusername
```

Η προτροπή αυτή είναι για να δώσουμε το όνομα χρήστη. Χρησιμοποιήστε το όνομα χρήστη που σας έχει δοθεί από τον ISP σας.

```
ISP Pass:mypassword
```

Η προτροπή αυτή είναι για τον κωδικό πρόσβασης. Απαντήστε με τον κωδικό που σας έχει δοθεί από τον ISP σας. Ο κωδικός αυτός δεν θα εμφανιστεί στην οθόνη σας, όπως ακριβώς συμβαίνει και με τον κωδικό σας όταν τον γράφετε στην προτροπή εισόδου του FreeBSD συστήματος σας.

```
Shell or PPP:ppp
```

Ανάλογα με τον ISP σας, μπορεί να μην δείτε και καθόλου την παραπάνω προτροπή. Στην παραπάνω περίπτωση μας ρωτάει αν επιθυμούμε να εκτελέσουμε κάποιο κέλυφος (shell) στο μηχάνημα του παροχέα, ή αν θέλουμε να εκκινήσουμε το ppp. Στο παράδειγμα μας επιλέξαμε να χρησιμοποιήσουμε ppp καθώς θέλουμε να συνδεθούμε στο Internet.

```
Ppp ON example>
```

Παρατηρήστε ότι στο παράδειγμα το πρώτο p είναι κεφαλαίο. Αυτό δείχνει ότι έχουμε συνδεθεί επιτυχώς με τον ISP.

```
PPp ON example>
```

Έχουμε πιστοποιηθεί με επιτυχία από τον ISP μας, και περιμένουμε να μας αποδοθεί διεύθυνση IP.

```
PPP ON example>
```

Έχει πλέον καθοριστεί διεύθυνση IP, και έχουμε ολοκληρώσει τη σύνδεση με επιτυχία.

```
PPP ON example>add default HISADDR
```

Εδώ προσθέτουμε την προεπιλεγμένη διαδρομή (default route). Το βήμα αυτό είναι απαραίτητο πριν μπορέσουμε να επικοινωνήσουμε με τον έξω κόσμο, καθώς τη δεδομένη στιγμή η μόνη σύνδεση που έχουμε είναι με ένα υπολογιστή από την άλλη μεριά της γραμμής. Αν το παραπάνω αποτύχει επειδή υπάρχουν ήδη καθορισμένες διαδρομές, μπορείτε να βάλετε ένα θαυμαστικό ! μπροστά από το add. Εναλλακτικά, μπορείτε να κάνετε αυτή τη ρύθμιση πριν επιχειρήσετε τη σύνδεση, και θα γίνει αυτόματα διαπραγμάτευση της νέας διαδρομής.

Αν όλα πήγαν καλά, θα πρέπει τώρα να έχετε ενεργή σύνδεση με το Internet, την οποία μπορείτε να μετακινήσετε στο παρασκήνιο χρησιμοποιώντας το συνδυασμό πλήκτρων CTRL + z. Αν παρατηρήσετε το PPP να γίνεται ξανά ppp, η σύνδεση έχει διακοπεί. Με τον τρόπο αυτό μπορείτε να παρακολουθείτε την κατάσταση της σύνδεση σας. Τα κεφαλαία P δείχνουν ότι υπάρχει σύνδεση με τον ISP ενώ τα μικρά p δείχνουν ότι για κάποιο λόγο η σύνδεση έχει χαθεί. Το ppp έχει μόνο αυτές τις δύο καταστάσεις.

52.4.2.1. Αντιμετώπιση Προβλημάτων

Αν έχετε απευθείας γραμμή και δεν φαίνεται να μπορείτε να αποκαταστήσετε τη σύνδεση, απενεργοποιήστε τον έλεγχο ροής μέσω υλικού (CTS/RTS) χρησιμοποιώντας την επιλογή `set ctsrts off`. Το παραπάνω συμβαίνει συνήθως αν είστε συνδεμένος σε κάποιο εξυπηρετητή τερματικών με δυνατότητα PPP, όπου το PPP σταματάει να αποκρίνεται όταν προσπαθεί να γράψει δεδομένα στη σύνδεση σας. Στην περίπτωση αυτή, συνήθως περιμένει για κάποιο σήμα CTS (Clear To Send) το οποίο δεν έρχεται ποτέ. Αν ωστόσο χρησιμοποιήσετε αυτή την επιλογή, θα πρέπει επίσης να χρησιμοποιήσετε και την επιλογή `set accmap` η οποία ενδεχομένως απαιτείται για να απομονωθεί το υλικό που εξαρτάται από τη μετάδοση συγκεκριμένων χαρακτήρων από τη μια άκρη στην άλλη, συνήθως μέσω του XON/XOFF. Δείτε τη σελίδα manual του ppp(8) για περισσότερες πληροφορίες σχετικά με αυτή την επιλογή και πως μπορείτε να την χρησιμοποιήσετε.

Αν διαθέτετε ένα παλαιότερο modem, ίσως χρειαστεί να χρησιμοποιήσετε την επιλογή `set parity even`. Η προεπιλεγμένη ρύθμιση είναι να μην υπάρχει ισοτιμία (parity none), αλλά σε παλιά modems (και σε κάποιους ISP) χρησιμοποιείται για έλεγχο λαθών (η χρήση της προκαλεί ωστόσο μεγάλη αύξηση στη μετακίνηση δεδομένων). Ίσως χρειαστείτε αυτή την επιλογή, αν ο ISP σας είναι η Compuserve.

Το PPP ίσως να μην επανέλθει στην κατάσταση εντολών, το οποίο είναι συνήθως σφάλμα διαπραγμάτευσης, καθώς ο ISP περιμένει από τη δική σας μεριά να ξεκινήσει τη διαπραγμάτευση. Στο σημείο αυτό, η χρήση της εντολής `~p` θα εξαναγκάσει το ppp να αρχίσει να στέλνει τις πληροφορίες σχετικά με τη ρύθμιση.

Αν δεν πάρετε ποτέ προτροπή εισόδου, το πιθανότερο είναι να πρέπει να χρησιμοποιήσετε πιστοποίηση PAP ή CHAP αντί για την τύπου UNIX® πιστοποίηση που περιγράψαμε στο παραπάνω παράδειγμα. Για να χρησιμοποιήσετε PAP ή CHAP απλώς προσθέστε τις παρακάτω επιλογές στην εφαρμογή PPP πριν βρεθείτε σε κατάσταση τερματικού:

```
ppp ON example> set authname myusername
```

Θα πρέπει να αντικαταστήσετε το *myusername* με το όνομα χρήστη που σας έχει δοθεί από τον ISP σας.

```
ppp ON example> set authkey mypassword
```

Θα πρέπει να αντικαταστήσετε το *mypassword* με τον κωδικό χρήστη που σας έχει δοθεί από τον ISP σας.

Αν συνδέεστε κανονικά, αλλά δεν φαίνεται να μπορείτε να επικοινωνήσετε με καμιά διεύθυνση, προσπαθήστε να χρησιμοποιήσετε την εντολή ping(8) με μια διεύθυνση IP για να δείτε αν θα λάβετε απάντηση. Αν βλέπετε απώλεια πακέτων 100%, το πιο πιθανό είναι ότι δεν έχετε καθορίσει κάποια προεπιλεγμένη διαδρομή. Ελέγξτε ξανά ότι έχετε ρυθμίσει την επιλογή `add default HISADDR` κατά τη διάρκεια της σύνδεσης. Αν μπορείτε να επικοινωνήσετε με μια απομακρυσμένη διεύθυνση IP, το πιθανότερο είναι ότι δεν έχετε βάλει τη διεύθυνση κάποιου διακομιστή ονομάτων στο αρχείο /etc/resolv.conf. Το αρχείο αυτό θα πρέπει να μοιάζει με το παρακάτω:

```
domain example.com
nameserver x.x.x.x
nameserver y.y.y.y
```

Όπου τα *x.x.x.x* και *y.y.y.y* θα πρέπει να αντικατασταθούν με τις διευθύνσεις IP των διακομιστών DNS του ISP σας. Ενδεχομένως οι πληροφορίες αυτές να σας έχουν δοθεί κατά την εγγραφή σας στην υπηρεσία. Αν όχι, θα μπορέσετε να τις βρείτε εύκολα με ένα τηλεφώνημα στον ISP σας.

Μπορείτε επίσης να ενεργοποιήσετε την καταγραφή συμβάντων για την PPP σύνδεση σας, μέσω του syslog(3). Απλώς προσθέστε:

```
!ppp
*.*     /var/log/ppp.log
```

στο /etc/syslog.conf. Τις περισσότερες φορές, αυτή η λειτουργία υπάρχει ήδη.

52.5. Χρησιμοποιώντας PPP μέσω Ethernet (PPPoE)

Η ενότητα αυτή περιγράφει πως να ρυθμίσετε μια σύνδεση PPP μέσω Ethernet (PPPoE).

52.5.1. Ρύθμιση του Πυρήνα

Δεν απαιτείται πλέον ειδική ρύθμιση του πυρήνα για τη λειτουργία PPPoE. Αν ο πυρήνας σας δεν περιλαμβάνει την απαραίτητη υποστήριξη netgraph, το ppp θα την φορτώσει αυτόματα ως άρθρωμα.

52.5.2. Ρύθμιση του ppp.conf

Παρακάτω φαίνεται ένα υπόδειγμα αρχείου ppp.conf:

```
default:
  set log Phase tun command # you can add more detailed logging if you wish
  set ifaddr 10.0.0.1/0 10.0.0.2/0

name_of_service_provider:
  set device PPPoE:xl1 # replace xl1 with your Ethernet device
  set authname YOURLOGINNAME
  set authkey YOURPASSWORD
  set dial
  set login
  add default HISADDR
```

52.5.3. Εκτέλεση του ppp

Ως χρήστης `root`, μπορείτε να εκτελέσετε:

```
# ppp -ddial name_of_service_provider
```

52.5.4. Εκκίνηση του ppp κατά την Εκκίνηση

Προσθέστε τις παρακάτω γραμμές στο αρχείο /etc/rc.conf:

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_nat="YES"   # if you want to enable nat for your local network, otherwise NO
ppp_profile="name_of_service_provider"
```

52.5.5. Χρήση μιας Ετικέτας Υπηρεσίας PPPoE

Μερικές φορές θα χρειαστεί να χρησιμοποιήσετε μια ετικέτα υπηρεσίας (service tag) για την αποκατάσταση της σύνδεσης σας. Οι ετικέτες υπηρεσιών χρησιμοποιούνται για τον διαχωρισμό μεταξύ διαφορετικών εξυπηρετητών PPPoE που βρίσκονται στο ίδιο δίκτυο.

Η τεκμηρίωση που σας έχει δώσει ο ISP σας, θα πρέπει να έχει τις απαιτούμενες πληροφορίες για την ετικέτα υπηρεσίας που χρειάζεστε. Αν δεν μπορείτε να την βρείτε, ρωτήστε την εξυπηρέτηση πελατών του ISP σας.

Ως τελευταία λύση, θα μπορούσατε να δοκιμάσετε την μέθοδο που συνίσταται στο πρόγραμμα Roaring Penguin PPPoE το οποίο μπορείτε να βρείτε στην Συλλογή των Ports. Να έχετε υπόψη σας, ότι αυτό μπορεί να αποπρογραμματίσει και να αχρηστεύσει το modem σας, έτσι σκεφτείτε το καλά πριν το κάνετε. Απλώς εγκαταστήστε το πρόγραμμα που δίνει ο παροχέας σας μαζί με το modem. Έπειτα, εισέλθετε στο μενού **System** του προγράμματος. Εκεί θα πρέπει να είναι το όνομα του προφίλ σας. Συνήθως γράφει *ISP*.

Το όνομα του προφίλ (ετικέτα υπηρεσίας) θα χρησιμοποιηθεί στην καταχώριση για την ρύθμιση του PPPoE στο αρχείο ppp.conf, ως το τμήμα που δηλώνει τον παροχέα στην εντολή `set device` (δείτε τη σελίδα manual του ppp(8) για πλήρεις λεπτομέρειες). Θα δείχνει όπως το παρακάτω:

```
set device PPPoE:xl1:ISP
```

Μην ξεχάσετε να αλλάξετε το *xl1* με τη σωστή συσκευή που αντιστοιχεί στην κάρτα Ethernet που χρησιμοποιείτε.

Μην ξεχάσετε να αλλάξετε το *ISP* με το προφίλ που βρήκατε παραπάνω.

Για περισσότερες πληροφορίες, δείτε:

- Φθηνότερες Ευρυζωνικές Συνδέσεις μέσω FreeBSD σε Γραμμή DSL από τον Renaud Waldura.

52.5.6. Το PPPoE σε Modem 3Com® HomeConnect™ ADSL Dual Link

Αυτό το modem δεν ακολουθεί το RFC 2516 (*Μια μέθοδος για μετάδοση PPP μέσω Ethernet (PPPoE)*,

γραμμένο από τους L. Mamakos, K. Lidl, J. Evarts, D. Carrel, D. Simone, και R. Wheeler). Αντίθετα, χρησιμοποιεί διαφορετικούς τύπους κωδικών πακέτων για τα πλαίσια Ethernet. Παρακαλούμε να εκφράσετε τα παράπονα σας στην 3Com αν νομίζετε ότι θα πρέπει να συμμορφωθεί με τις προδιαγραφές του PPPoE.

Για να μπορεί το FreeBSD να επικοινωνεί με αυτή τη συσκευή, θα πρέπει να τεθεί ένα κατάλληλο sysctl. Αυτό μπορεί να γίνεται αυτόματα κατά την εκκίνηση, με την ενημέρωση του αρχείου /etc/sysctl.conf:

```
net.graph.nonstandard_pppoe=1
```

ή μπορεί να γίνει άμεσα με την εντολή:

```
# sysctl net.graph.nonstandard_pppoe=1
```

Δυστυχώς, επειδή πρόκειται για μια ρύθμιση που επηρεάζει ολόκληρο το σύστημα, δεν είναι δυνατόν να επικοινωνείτε ταυτόχρονα με ένα κανονικό πελάτη ή εξυπηρετητή PPPoE και με ένα ADSL modem 3Com® HomeConnect™.

52.6. Χρησιμοποιώντας PPP μέσω ATM (PPPoA)

Η ενότητα που ακολουθεί, περιγράφει πως να ρυθμίσετε το PPP για λειτουργία μέσω ATM (PPPoA). Το PPPoA είναι μια δημοφιλής επιλογή στους παροχείς υπηρεσιών DSL στην Ευρώπη.

52.6.1. Χρησιμοποιώντας PPPoA με το Alcatel SpeedTouch™ USB

Η υποστήριξη PPPooA για αυτή τη συσκευή, παρέχεται ως port στο FreeBSD, καθώς το firmware της συσκευής διανέμεται υπό την άδεια Alcatel's license agreement και δεν μπορεί να διανεμηθεί ελεύθερα με το βασικό σύστημα του FreeBSD.

Για να εγκαταστήσετε το λογισμικό, απλά χρησιμοποιήστε την Συλλογή των Ports. Εγκαταστήστε το port net/pppoa και ακολουθήστε τις οδηγίες που περιλαμβάνονται σε αυτό.

Όπως πολλές συσκευές USB, το Alcatel SpeedTouch™ χρειάζεται να κατεβάσει το firmware του από τον υπολογιστή στο οποίο είναι συνδεμένο, προκειμένου να λειτουργήσει σωστά. Η διαδικασία αυτή μπορεί να αυτοματοποιηθεί στο FreeBSD, ώστε η μεταφορά να γίνεται κάθε φορά που συνδέεται η συσκευή στη θύρα USB. Μπορείτε να προσθέσετε τις παρακάτω πληροφορίες στο αρχείο /etc/usbd.conf για να ενεργοποιήσετε την αυτόματη μεταφορά του firmware. Θα πρέπει να επεξεργαστείτε αυτό το αρχείο ως χρήστης `root`.

```
device "Alcatel SpeedTouch USB"
    devname "ugen[0-9]+"
    vendor 0x06b9
    product 0x4061
    attach "/usr/local/sbin/modem_run -f /usr/local/libdata/mgmt.o"
```

Για να ενεργοποιήσετε το usbd, το δαίμονα USB, προσθέστε την παρακάτω γραμμή στο αρχείο /etc/rc.conf:

```
usbd_enable="YES"
```

Μπορεί επίσης να ρυθμίσετε το ppp ώστε να εκτελεί αυτόματα κλήση κατά την εκκίνηση του συστήματος. Για να γίνει αυτό, προσθέστε τις παρακάτω γραμμές στο /etc/rc.conf. Θα πρέπει και πάλι να εκτελέσετε τη διαδικασία αυτή ως `root`.

```
ppp_enable="YES"
ppp_mode="ddial"
ppp_profile="adsl"
```

Για να λειτουργήσει σωστά το παραπάνω, θα πρέπει να έχετε χρησιμοποιήσει το υπόδειγμα του αρχείου ppp.conf το οποίο παρέχεται με το port net/pppoa.

52.6.2. Χρησιμοποιώντας το mpd

Μπορείτε να χρησιμοποιήσετε το mpd για να συνδεθείτε σε ένα πλήθος υπηρεσιών, και ειδικότερα υπηρεσίες PPTP. Μπορείτε να βρείτε το mpd στην Συλλογή των Ports, στο net/mpd. Πολλά ADSL modem απαιτούν τη δημιουργία ενός PPTP τούνελ μεταξύ του modem και του υπολογιστή. Ένα τέτοιο modem είναι το Alcatel SpeedTouch™ Home.

Πρώτα πρέπει να εγκαταστήσετε το port, και μετά μπορείτε να ρυθμίσετε το mpd ώστε να καλύπτει τις απαιτήσεις σας και τις ρυθμίσεις του παροχέα σας. Το port εγκαθιστά κάποια παραδείγματα αρχείων ρυθμίσεων στον κατάλογο PREFIX/etc/mpd/. Τα αρχεία αυτά περιέχουν αρκετά καλή τεκμηρίωση των ρυθμίσεων. Σημειώστε εδώ, ότι το *PREFIX* είναι ο κατάλογος στον οποίο εγκαθίστανται τα ports, και από προεπιλογή είναι ο /usr/local/. Μετά την εγκατάσταση του port, θα βρείτε ένα πλήρη οδηγό για τη ρύθμιση του mpd σε μορφή HTML. Η τεκμηρίωση εγκαθίσταται στον κατάλογο PREFIX/shared/doc/mpd/. Παρακάτω φαίνεται ένα υπόδειγμα ρυθμίσεων για σύνδεση σε μια υπηρεσία ADSL μέσω του mpd. Οι ρυθμίσεις χωρίζονται σε δύο αρχεία, πρώτα δείχνουμε το mpd.conf:

Το παρακάτω υπόδειγμα mpd.conf λειτουργεί μόνο με την έκδοση 4.X του mpd.

```
default:
    load adsl

adsl:
    new -i ng0 adsl adsl
    set bundle authname username ①
    set bundle password password ②
    set bundle disable multilink

    set link no pap acfcomp protocomp
    set link disable chap
```

```
    set link accept chap
    set link keep-alive 30 10

    set ipcp no vjcomp
    set ipcp ranges 0.0.0.0/0 0.0.0.0/0

    set iface route default
    set iface disable on-demand
    set iface enable proxy-arp
    set iface idle 0

    open
```

① Το όνομα χρήστη με το οποίο γίνεται η πιστοποίηση στον ISP σας.

② Ο κωδικός με τον οποίο γίνεται η πιστοποίηση στον ISP σας.

Το αρχείο mpd.links περιέχει πληροφορίες σχετικά με τη σύνδεση ή τις συνδέσεις που θα πραγματοποιηθούν. Για παράδειγμα, το mpd.links που συνοδεύει το παραπάνω παράδειγμα, φαίνεται παρακάτω:

```
adsl:
    set link type pptp
    set pptp mode active
    set pptp enable originate outcall
    set pptp self 10.0.0.1 ①
    set pptp peer 10.0.0.138 ②
```

① Η διεύθυνση IP του FreeBSD υπολογιστή σας, στον οποίο θα χρησιμοποιήσετε το mpd.

② Η διεύθυνση IP του ADSL modem σας. Για το Alcatel SpeedTouch™ Home, η διεύθυνση αυτή είναι από προεπιλογή η `10.0.0.138`.

Είναι δυνατόν να αρχικοποιήσετε τη σύνδεση εύκολα, δίνοντας την παρακάτω εντολή ως `root`:

```
# mpd -b adsl
```

Μπορείτε να δείτε την κατάσταση της σύνδεσης με την παρακάτω εντολή:

```
% ifconfig ng0
ng0: flags=88d1<UP,POINTOPOINT,RUNNING,NOARP,SIMPLEX,MULTICAST> mtu 1500
     inet 216.136.204.117 --> 204.152.186.171 netmask 0xffffffff
```

Το mpd αποτελεί τον συνιστώμενο τρόπο σύνδεσης του FreeBSD με μια υπηρεσία ADSL.

52.6.3. Χρησιμοποιώντας το pptpclient

Μπορείτε επίσης να χρησιμοποιήσετε το FreeBSD για να συνδεθείτε σε άλλες υπηρεσίες PPPoA

χρησιμοποιώντας το net/pptpclient.

Για να χρησιμοποιήσετε το net/pptpclient για να συνδεθείτε σε μια υπηρεσία DSL, εγκαταστήστε το port ή το πακέτο, και επεξεργαστείτε το αρχείο /etc/ppp/ppp.conf. Θα χρειαστεί να είστε `root` για να κάνετε και τις δύο παραπάνω διαδικασίες. Παρακάτω φαίνεται ένα παράδειγμα μιας ενότητας του ppp.conf. Για περισσότερες πληροφορίες σχετικά με τις επιλογές του ppp.conf, δείτε τη σελίδα manual του ppp, ppp(8).

```
adsl:
 set log phase chat lcp ipcp ccp tun command
 set timeout 0
 enable dns
 set authname username ①
 set authkey password ②
 set ifaddr 0 0
 add default HISADDR
```

① Το όνομα χρήστη για τον λογαριασμό σας στον παροχέα DSL.

② Ο κωδικός για τον λογαριασμό σας.

Καθώς θα πρέπει να γράψετε τον κωδικό σας μορφή απλού κειμένου στο αρχείο ppp.conf, θα πρέπει να βεβαιωθείτε ότι κανένας άλλος δεν θα μπορεί να διαβάσει τα περιεχόμενα αυτού του αρχείου. Με τις παρακάτω εντολές, μπορείτε να εξασφαλίσετε ότι το αρχείο θα μπορεί να διαβαστεί μόνο μέσα από το λογαριασμό του `root`. Δείτε τις σελίδες manual των chmod(1) και chown(8) για περισσότερες πληροφορίες.

```
# chown root:wheel /etc/ppp/ppp.conf
# chmod 600 /etc/ppp/ppp.conf
```

Αυτό θα ανοίξει ένα τούνελ για μια συνεδρία PPP με τον DSL δρομολογητή σας. Τα DSL modem τύπου ethernet έχουν μια προκαθορισμένη διεύθυνση IP στο τοπικό σας δίκτυο, στην οποία μπορείτε να συνδεθείτε. Στην περίπτωση του Alcatel SpeedTouch™ Home, η διεύθυνση αυτή είναι `10.0.0.138`. Η τεκμηρίωση που διαθέτει ο δρομολογητής σας, θα αναφέρει ποια διεύθυνση χρησιμοποιεί η συσκευή σας. Για να ανοίξετε το τούνελ και να ξεκινήσετε μια συνεδρία PPP, εκτελέστε την ακόλουθη εντολή:

```
# pptp address adsl
```

Είναι καλή ιδέα να προσθέσετε ένα "&" στο τέλος της προηγούμενης εντολής, διαφορετικά το pptp δεν θα σας επιστρέψει τον έλεγχο (προτροπή) του τερματικού σας.

Θα δημιουργηθεί μια συσκευή tun (εικονικό τούνελ) για την αλληλεπίδραση μεταξύ των διεργασιών pptp και ppp. Μόλις επιστρέψει η προτροπή στο τερματικό σας, ή το pptp επιβεβαιώσει τη σύνδεση,

μπορείτε να εξετάσετε το τούνελ με τον τρόπο που φαίνεται παρακάτω:

```
% ifconfig tun0
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        inet 216.136.204.21 --> 204.152.186.171 netmask 0xffffff00
        Opened by PID 918
```

Αν δεν μπορέσετε να συνδεθείτε, ελέγξτε τις ρυθμίσεις του δρομολογητή σας, οι οποίες συνήθως είναι προσβάσιμες μέσω telnet ή μέσω κάποιου φυλλομετρητή. Αν ακόμα δεν μπορείτε να συνδεθείτε, θα πρέπει να εξετάσετε την έξοδο της εντολής `pptp` και τα περιεχόμενα του αρχείου καταγραφής του ppp, /var/log/ppp.log για πιθανά στοιχεία.

52.7. Χρησιμοποιώντας το SLIP

Η ενότητα αυτή εφαρμόζεται και είναι έγκυρη μόνο σε συστήματα FreeBSD 7.X.

52.7.1. Ρυθμίζοντας ένα Πελάτη SLIP

Παρακάτω παρουσιάζουμε ένα τρόπο να ρυθμίσετε ένα μηχάνημα FreeBSD ως πελάτη SLIP σε ένα δίκτυο με στατικές διευθύνσεις. Για μηχανήματα τα οποία λαμβάνουν όνομα δυναμικά (η διεύθυνση τους αλλάζει κάθε φορά που συνδέονται), πιθανόν να χρειαστεί να κάνετε πιο πολύπλοκες ρυθμίσεις.

Αρχικά, θα πρέπει να καθορίσετε σε ποια σειριακή θύρα είναι συνδεμένο το modem σας. Αρκετοί χρήστες δημιουργούν ένα συμβολικό δεσμό π.χ. /dev/modem, το οποίο δείχνει στην πραγματική συσκευή /dev/cuadN. Αυτό σας επιτρέπει να συνεχίσετε να χρησιμοποιείτε το ίδιο όνομα συσκευής, ακόμα και αν μετακινήσετε το modem σε διαφορετική θύρα. Είναι μάλλον άβολο να πρέπει να αλλάξετε πλήθος αρχείων στο /etc καθώς και τα αρχεία .kermrc σε όλο το σύστημα!

Το /dev/cuad0 είναι η COM1, το /dev/cuad1 είναι η COM2, κ.ο.κ.

Βεβαιωθείτε ότι το αρχείο ρυθμίσεων του πυρήνα σας περιέχει τα παρακάτω:

```
device   sl
```

Το παραπάνω περιλαμβάνεται στον πυρήνα GENERIC, και αν δεν το έχετε διαγράψει, δεν θα έχετε πρόβλημα.

52.7.1.1. Ρυθμίσεις που θα Χρειαστεί να Κάνετε Μόνο μια Φορά

1. Προσθέστε το μηχάνημα σας, την πύλη (gateway) και τους διακομιστές ονομάτων (nameservers) στο αρχείο /etc/hosts. Στο παράδειγμα μας, το αρχείο αυτό μοιάζει με το παρακάτω:

   ```
   127.0.0.1               localhost loghost
   136.152.64.181          water.CS.Example.EDU water.CS water
   136.152.64.1            inr-3.CS.Example.EDU inr-3 slip-gateway
   ```

```
128.32.136.9            ns1.Example.EDU ns1
128.32.136.12           ns2.Example.EDU ns2
```

2. Βεβαιωθείτε ότι η ενότητα `files` βρίσκεται πριν το `dns` στην ενότητα `hosts:` του αρχείου /etc/nsswitch.conf. Αν δεν υπάρχουν αυτές οι παράμετροι, μπορεί να εμφανιστούν παράξενα συμπτώματα.
3. Τροποποιήστε το αρχείο /etc/rc.conf.
   a. Ορίστε το όνομα του υπολογιστή σας, τροποποιώντας τη γραμμή που γράφει:

   ```
   hostname="myname.my.domain"
   ```

   Θα πρέπει εδώ να τοποθετήσετε το πλήρες όνομα του υπολογιστή σας.

   b. Ορίστε τον προεπιλεγμένο δρομολογητή, αλλάζοντας τη γραμμή:

   ```
   defaultrouter="NO"
   ```

   σε:

   ```
   defaultrouter="slip-gateway"
   ```

4. Δημιουργήστε ένα αρχείο /etc/resolv.conf το οποίο θα περιέχει:

```
domain CS.Example.EDU
nameserver 128.32.136.9
nameserver 128.32.136.12
```

Όπως μπορείτε να δείτε, το παραπάνω ορίζει τους διακομιστές DNS. Φυσικά, τα πραγματικά ονόματα και οι διευθύνσεις των τομέων εξαρτώνται από το περιβάλλον σας.

5. Ρυθμίστε κωδικό πρόσβασης για τους χρήστες `root` και `toor` (καθώς και για όσους άλλους λογαριασμούς δεν έχουν κωδικό).
6. Επανεκκινήστε το μηχάνημα σας, και βεβαιωθείτε ότι έχει τεθεί σωστά το όνομα υπολογιστή.

52.7.1.2. Δημιουργώντας μια Σύνδεση SLIP

1. Μετά την κλήση, γράψτε την εντολή `slip` στην προτροπή, γράψτε το όνομα του μηχανήματος σας και τον κωδικό. Το τι ακριβώς χρειάζεται να γράψετε, εξαρτάται από το περιβάλλον σας. Αν χρησιμοποιείτε το Kermit, μπορείτε να χρησιμοποιήσετε ένα script όπως το ακόλουθο:

```
# kermit setup
set modem hayes
set line /dev/modem
set speed 115200
```

```
set parity none
set flow rts/cts
set terminal bytesize 8
set file type binary
# The next macro will dial up and login
define slip dial 643-9600, input 10 =>, if failure stop, -
output slip\x0d, input 10 Username:, if failure stop, -
output silvia\x0d, input 10 Password:, if failure stop, -
output ***\x0d, echo \x0aCONNECTED\x0a
```

Φυσικά, θα πρέπει να αλλάξετε το όνομα χρήστη και τον κωδικό ώστε να ταιριάζουν με τα δικά σας. Μετά από αυτό, μπορείτε απλώς να πληκτρολογήσετε `slip` στην προτροπή σύνδεσης του Kermit.

Η ύπαρξη του κωδικού σας σε μορφή απλού κειμένου σε οποιοδήποτε σημείο ενός συστήματος αρχείων, είναι γενικά *κακή* ιδέα. Προχωρήστε με δική σας ευθύνη.

2. Αφήστε το Kermit εκεί (μπορείτε να το στείλετε στο παρασκήνιο χρησιμοποιώντας τα πλήκτρα `Ctrl` + `z`) και ως `root`, γράψτε:

```
# slattach -h -c -s 115200 /dev/modem
```

Αν μπορείτε να κάνετε `ping` σε υπολογιστές στην άλλη μεριά του δρομολογητή, είστε συνδεμένοι! Αν αυτό δεν δουλεύει, δοκιμάστε την επιλογή `-a` αντί για την `-c` ως όρισμα στην `slattach`.

52.7.1.3. Πως να Τερματίσετε την Σύνδεση

Κάντε τα ακόλουθα:

```
# kill -INT `cat /var/run/slattach.modem.pid`
```

για να τερματίσετε το `slattach`. Θυμηθείτε ότι πρέπει να είστε `root` για να εκτελέσετε το παραπάνω. Έπειτα επανέλθετε στο `kermit` (εκτελώντας την `fg` αν το είχατε στείλει στο παρασκήνιο) και τερματίστε το (πιέζοντας `q`).

Η σελίδα manual του slattach(8) αναφέρει ότι μπορείτε να χρησιμοποιήσετε την εντολή `ifconfig sl0 down` για να διακόψετε τη σύνδεση, αλλά αυτό δεν φαίνεται να έχει κανένα αποτέλεσμα. (Το `ifconfig sl0` αναφέρει το ίδιο πράγμα.)

Μερικές φορές, το modem σας μπορεί να αρνηθεί να κλείσει τη γραμμή. Στις περιπτώσεις αυτές, ξεκινήστε ξανά το `kermit` και τερματίστε το ξανά. Τη δεύτερη φορά συνήθως πετυχαίνει.

52.7.1.4. Αντιμετώπιση Προβλημάτων

Αν το παραπάνω δεν λειτουργήσει, ρωτήστε στη λίστα freebsd-net. Μερικά από τα συνηθισμένα

προβλήματα τα οποία έχουμε μέχρι στιγμής αντιμετωπίσει:

- Να μην έχει χρησιμοποιηθεί η επιλογή `-c` ή `-a` στην `slattach` (Αυτό κανονικά δεν είναι κρίσιμο σφάλμα, αλλά μερικοί χρήστες ανέφεραν ότι αυτό έλυσε τα προβλήματα τους.)
- Χρήση του `s10` αντί για `sl0` (η διαφορά μπορεί να είναι πολύ μικρή σε μερικές γραμματοσειρές).
- Δοκιμάστε την εντολή `ifconfig sl0` για να δείτε την κατάσταση της διεπαφής. Για παράδειγμα, μπορεί να δείτε το παρακάτω:

```
# ifconfig sl0
sl0: flags=10<POINTOPOINT>
        inet 136.152.64.181 --> 136.152.64.1 netmask ffffff00
```

- Αν η εντολή ping(8) δίνει μηνύματα `no route to host`, ίσως υπάρχει πρόβλημα με τον πίνακα δρομολόγησης σας. Μπορείτε να χρησιμοποιήσετε την εντολή `netstat -r` για να δείτε την τρέχουσα δρομολόγηση:

```
# netstat -r
Routing tables
Destination      Gateway            Flags     Refs     Use  IfaceMTU    Rtt
Netmasks:

(root node)
(root node)

Route Tree for Protocol Family inet:
(root node) =>
default          inr-3.Example.EDU  UG          8   224515  sl0 -      -
localhost.Exampl localhost.Example. UH          5    42127  lo0 -       0.438
inr-3.Example.ED water.CS.Example.E UH          1        0  sl0 -      -
water.CS.Example localhost.Example. UGH        34 47641234  lo0 -       0.438
(root node)
```

Τα παραπάνω παραδείγματα είναι από ένα σχετικά απασχολημένο σύστημα. Οι αριθμοί θα διαφέρουν στο σύστημα σας, ανάλογα με τη δραστηριότητα του δικτύου.

52.7.2. Ρυθμίζοντας Ένα Εξυπηρετητή SLIP

Το κείμενο αυτό παρέχει κάποιες υποδείξεις για τη ρύθμιση ενός FreeBSD συστήματος ως εξυπηρετητή SLIP. Τυπικά αυτό σημαίνει ότι το σύστημα σας θα ρυθμιστεί να ξεκινά αυτόματα τις συνδέσεις μετά την είσοδο απομακρυσμένων πελατών SLIP.

52.7.2.1. Προϋποθέσεις

Η ενότητα αυτή είναι ιδιαίτερα τεχνικής φύσεως, και για το λόγο αυτό απαιτείται να έχετε τις αντίστοιχες γνώσεις για να την κατανοήσετε. Υποθέτουμε ότι έχετε μια εξοικείωση με το πρωτόκολλο TCP/IP και ειδικότερα με τη διευθυνσιοδότηση κόμβων, τις μάσκες δικτύων, τα υποδίκτυα, τη δρομολόγηση και τα πρωτόκολλα δρομολόγησης όπως το RIP. Η ρύθμιση των

υπηρεσιών SLIP σε ένα εξυπηρετητή επιλογικών συνδέσεων απαιτεί γνώση αυτών των εννοιών, και αν δεν είστε εξοικειωμένος με αυτές, σας παρακαλούμε να διαβάσετε είτε το *TCP/IP Network Administration* του Craig Hunt (εκδόσεις O'Reilly & Associates, Inc, Αριθμός ISBN 0-937175-82-X) ή κάποιο από τα βιβλία του Douglas Comer σχετικά με το πρωτόκολλο TCP/IP.

Επιπλέον, υποθέτουμε ότι ήδη έχετε ρυθμίσει το modem σας και έχετε τροποποιήσει τα κατάλληλα αρχεία ρυθμίσεων του συστήματος ώστε να επιτρέπεται η είσοδος στο σύστημα μέσω των modem. Αν δεν έχετε ακόμα προετοιμάσει το σύστημα για αυτό, παρακαλούμε δείτε το Υπηρεσία Εισόδου μέσω Επιλογικής Σύνδεσης (dial-in) για λεπτομέρειες σχετικά με τη ρύθμιση των επιλογικών συνδέσεων. Ενδεχομένως να θέλετε επίσης να δείτε τις σελίδες manual της sio(4) για πληροφορίες σχετικά με το πρόγραμμα οδήγησης της σειριακής θύρας, τα ttys(5), gettytab(5), getty(8), και init(8) για πληροφορίες που σχετίζονται με τη ρύθμιση του συστήματος ώστε να δέχεται είσοδο χρηστών μέσω modem, και ίσως και τη stty(1) για πληροφορίες σχετικά με τις παραμέτρους σειριακών θυρών (όπως την `clocal` για σειριακές διεπαφές που είναι απευθείας συνδεμένες).

52.7.2.2. Γρήγορη Επισκόπηση

Τυπικά, ένας εξυπηρετητής SLIP που χρησιμοποιεί FreeBSD λειτουργεί με τον εξής τρόπο: ένας χρήστης SLIP καλεί τον εξυπηρετητή SLIP, και εισέρχεται στο σύστημα μέσω ενός ειδικού αναγνωριστικού εισόδου για το SLIP. Το κέλυφος του χρήστη είναι το /usr/sbin/sliplogin. Το πρόγραμμα `sliplogin` διαβάζει το αρχείο /etc/sliphome/slip.hosts για να βρει μια γραμμή που να ταιριάζει με τον χρήστη, και αν υπάρχει, συνδέει την σειριακή γραμμή σε μια διαθέσιμη διεπαφή SLIP και έπειτα εκτελεί το script του κελύφους /etc/sliphome/slip.login για να ρυθμίσει τη διεπαφή SLIP.

52.7.2.2.1. Ένα Παράδειγμα Εισόδου σε Εξυπηρετητή SLIP

Για παράδειγμα, για ένα χρήστη SLIP με ID `Shelmerg`, η αντίστοιχη καταχώριση στο /etc/master.passwd θα έμοιαζε με την παρακάτω:

```
Shelmerg:password:1964:89::0:0:Guy Helmer -
SLIP:/usr/users/Shelmerg:/usr/sbin/sliplogin
```

Όταν εισέλθει ο `Shelmerg`, το `sliplogin` θα ψάξει το /etc/sliphome/slip.hosts για μια γραμμή με ID χρήστη που να ταιριάζει. Για παράδειγμα, μπορεί να υπάρχει μια γραμμή στο /etc/sliphome/slip.hosts που να γράφει:

```
Shelmerg        dc-slip sl-helmer       0xfffffc00      autocomp
```

Το `sliplogin` θα βρει τη γραμμή αυτή, θα συνδέσει τη σειριακή γραμμή στην επόμενη διαθέσιμη διεπαφή SLIP, και έπειτα θα εκτελέσει το /etc/sliphome/slip.login όπως φαίνεται παρακάτω:

```
/etc/sliphome/slip.login 0 19200 Shelmerg dc-slip sl-helmer 0xfffffc00 autocomp
```

Αν όλα πάνε καλά, το /etc/sliphome/slip.login θα εκτελέσει μια εντολή `ifconfig` για τη διεπαφή SLIP στην οποία έχει συνδεθεί η `sliplogin` (η διεπαφή 0 στο παραπάνω παράδειγμα, η πρώτη παράμετρος

της λίστας που δίνεται στο slip.login) ώστε να ρυθμιστούν η τοπική διεύθυνση IP (`dc-slip`), η απομακρυσμένη διεύθυνση IP (`sl-helmer`), η μάσκα δικτύου για τη διεπαφή SLIP (`0xffffc00`), και οποιεσδήποτε πρόσθετες επιλογές (`autocomp`). Αν κάτι πάει στραβά, θα μπορέσετε να το εντοπίσετε από τα αρχεία καταγραφής της `sliplogin`. Η `sliplogin` καταγράφει τα μηνύματα χρησιμοποιώντας το δαίμονα syslogd ο οποίος συνήθως χρησιμοποιεί το αρχείο /var/log/messages (δείτε τις σελίδες βοήθειας για τα syslogd(8) και syslog.conf(5) και ενδεχομένως ελέγξτε το /etc/syslog.conf για να δείτε την τοποθεσία και το αρχείο που χρησιμοποιεί το syslogd για την καταγραφή).

52.7.2.3. Ρύθμιση του Πυρήνα

Ο προεπιλεγμένος πυρήνας του FreeBSD (ο GENERIC) διαθέτει ενσωματωμένη υποστήριξη SLIP (sl(4)). Στην περίπτωση που θέλετε να δημιουργήσετε προσαρμοσμένο πυρήνα, προσθέστε την παρακάτω γραμμή στο αρχείο ρυθμίσεων του πυρήνα σας:

```
device   sl
```

Το FreeBSD, από προεπιλογή, δεν προωθεί πακέτα. Αν θέλετε ο εξυπηρετητής σας να ενεργεί ως δρομολογητής, θα πρέπει να επεξεργαστείτε το αρχείο /etc/rc.conf και να αλλάξετε τη ρύθμιση της μεταβλητής `gateway_enable` σε `YES`. Με τον τρόπο αυτό, θα είναι σίγουρο ότι η επιλογή της δρομολόγησης θα διατηρηθεί μετά από μια επανεκκίνηση.

Θα πρέπει έπειτα να επανεκκινήσετε για να ενεργοποιηθούν οι νέες ρυθμίσεις.

Για να εφαρμόσετε αυτές τις ρυθμίσεις άμεσα, μπορείτε να εκτελέσετε την παρακάτω εντολή ως `root`:

```
# /etc/rc.d/routing start
```

Παρακαλούμε δείτε το Ρυθμίζοντας τον Πυρήνα του FreeBSD για περισσότερες πληροφορίες σχετικά με την ρύθμιση του πυρήνα του FreeBSD.

52.7.2.4. Ρύθμιση του Sliplogin

Όπως αναφέρθηκε και πριν, υπάρχουν τρία αρχεία στον κατάλογο /etc/sliphome τα οποία χρησιμοποιούνται στη ρύθμιση του /usr/sbin/sliplogin (δείτε και τη σελίδα manual του sliplogin(8)): το slip.hosts, το οποίο ορίζει τους χρήστες SLIP και τις αντίστοιχες IP διευθύνσεις τους, το slip.login το οποίο συνήθως ρυθμίζει απλά την διεπαφή SLIP, και προαιρετικά το slip.logout, το οποίο αναιρεί τις αλλαγές του slip.login όταν τερματίσει η σειριακή σύνδεση.

52.7.2.4.1. Ρύθμιση του slip.hosts

Το /etc/sliphome/slip.hosts περιέχει γραμμές με τέσσερα πεδία που χωρίζονται μεταξύ τους με κενά διαστήματα:

- Το αναγνωριστικό εισόδου του χρήστη SLIP
- Την τοπική διεύθυνση (τοπική ως προς τον εξυπηρετητή SLIP) της διασύνδεσης SLIP
- Την απομακρυσμένη διεύθυνση της διασύνδεσης SLIP

- Τη μάσκα του δικτύου

Η τοπική και η απομακρυσμένη διεύθυνση, μπορεί να είναι ονόματα υπολογιστών (τα οποία να μετατρέπονται σε διευθύνσεις IP μέσω του /etc/hosts ή μέσω του DNS, ανάλογα με τις καταχωρίσεις που υπάρχουν στο αρχείο /etc/nsswitch.conf), και η μάσκα δικτύου μπορεί να είναι ένα όνομα το οποίο να μπορεί να διευκρινιστεί μέσω αναζήτησης στο /etc/networks. Σε ένα δοκιμαστικό σύστημα, το /etc/sliphome/slip.hosts μοιάζει με το παρακάτω:

```
#
# login local-addr      remote-addr     mask            opt1    opt2
#                                                (normal,compress,noicmp)
#
Shelmerg  dc-slip       sl-helmerg      0xfffffc00      autocomp
```

Στο τέλος της γραμμής, βρίσκονται μια ή περισσότερες από τις παρακάτω επιλογές:

- `normal` - χωρίς συμπίεση των επικεφαλίδων
- `compress` - με συμπίεση των επικεφαλίδων
- `autocomp` - με συμπίεση των επικεφαλίδων, αν επιτρέπεται από τον απομακρυσμένο υπολογιστή
- `noicmp` - απενεργοποίηση των πακέτων ICMP (με τον τρόπο αυτό τα πακέτα "ping" θα απορρίπτονται αντί να καταναλώνουν το εύρος ζώνης της σύνδεσης σας)

Οι επιλογές που έχετε για τις τοπικές και απομακρυσμένες διευθύνσεις των SLIP συνδέσεων σας, εξαρτώνται από το αν πρόκειται να αφιερώσετε ένα υποδίκτυο TCP/IP ή αν πρόκειται να χρησιμοποιήσετε "proxy ARP" στο SLIP εξυπηρετητή σας (δεν είναι "πραγματικό" proxy ARP, αλλά στην ενότητα αυτή περιγράφεται με αυτό τον όρο). Αν δεν είστε σίγουρος ποια μέθοδο να επιλέξετε ή πως να αποδίδετε διευθύνσεις IP, παρακαλούμε ανατρέξτε στα βιβλία του TCP/IP που αναφέρονται στις Προϋποθέσεις SLIP (Προϋποθέσεις) ή/και συμβουλευθείτε το διαχειριστή δικτύου σας.

Αν πρόκειται να χρησιμοποιήσετε ξεχωριστό υποδίκτυο για τους SLIP πελάτες σας, θα χρειαστεί να διαθέσετε τον αριθμό υποδικτύου από την διεύθυνση IP που σας έχει αποδοθεί και να αποδώσετε στους πελάτες SLIP διευθύνσεις που ανήκουν σε αυτό το υποδίκτυο. Έπειτα, θα χρειαστεί μάλλον να καθορίσετε μια στατική διαδρομή στο υποδίκτυο SLIP μέσω του εξυπηρετητή SLIP στον κοντινότερο σας δρομολογητή IP.

Διαφορετικά, αν χρησιμοποιήσετε τη μέθοδο "proxy ARP", θα χρειαστεί να αποδίδετε στους SLIP πελάτες σας διευθύνσεις IP που ανήκουν στο υποδίκτυο Ethernet στο οποίο ανήκει ο εξυπηρετητής SLIP, και θα χρειαστεί επίσης να ρυθμίσετε τα scripts /etc/sliphome/slip.login και /etc/sliphome/slip.logout να χρησιμοποιούν το arp(8) για να χειρίζονται τις καταχωρίσεις "proxy ARP" στον πίνακα ARP του εξυπηρετητή SLIP.

52.7.2.4.2. Ρύθμιση του slip.login

Ένα τυπικό /etc/sliphome/slip.login μοιάζει με το παρακάτω:

```
#!/bin/sh -
#
```

```
#       @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# generic login file for a slip line.  sliplogin invokes this with
# the parameters:
#      1        2         3        4          5         6     7-n
#   slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
```

Το αρχείο slip.login εκτελεί απλώς το `ifconfig` για την κατάλληλη διεπαφή SLIP, με τις τοπικές και απομακρυσμένες διευθύνσεις και τη μάσκα δικτύου της διεπαφής αυτής.

Αν έχετε αποφασίσει να χρησιμοποιήσετε την μέθοδο "proxy ARP" (αντί να χρησιμοποιήσετε διαφορετικό υποδίκτυο για τους πελάτες SLIP), το αρχείο /etc/sliphome/slip.login θα μοιάζει με το παρακάτω:

```
#!/bin/sh -
#
#       @(#)slip.login  5.1 (Berkeley) 7/1/90

#
# generic login file for a slip line.  sliplogin invokes this with
# the parameters:
#      1        2         3        4          5         6     7-n
#   slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 inet $4 $5 netmask $6
# Answer ARP requests for the SLIP client with our Ethernet addr
/usr/sbin/arp -s $5 00:11:22:33:44:55 pub
```

Η πρόσθετη γραμμή σε αυτό το slip.login, η `arp -s $5 00:11:22:33:44:55 pub`, δημιουργεί μια καταχώριση ARP στον πίνακα ARP του εξυπηρετητή SLIP. Αυτή η καταχώριση ARP κάνει τον εξυπηρετητή SLIP να απαντά με την διεύθυνση Ethernet MAC όταν κάποιος άλλος κόμβος IP στο Ethernet επιθυμεί να επικοινωνήσει με την διεύθυνση IP του πελάτη SLIP.

Όταν χρησιμοποιείτε το παραπάνω παράδειγμα, βεβαιωθείτε ότι έχετε αντικαταστήσει την διεύθυνση MAC του Ethernet (`00:11:22:33:44:55`) με την αντίστοιχη της δικής σας κάρτας Ethernet, διαφορετικά το "proxy ARP" σίγουρα δεν θα λειτουργήσει! Μπορείτε να ανακαλύψετε τη διεύθυνση MAC του δικού σας εξυπηρετητή SLIP κοιτάζοντας τα αποτελέσματα της εντολής `netstat -i`. Η δεύτερη γραμμή της εξόδου θα μοιάζει με την παρακάτω:

```
ed0   1500  <Link>0.2.c1.28.5f.4a         191923    0   129457     0   116
```

Αυτό δείχνει ότι στο συγκεκριμένο σύστημα η διεύθυνση MAC του Ethernet είναι `00:02:c1:28:5f:4a`. Οι τελείες στην διεύθυνση που δείχνει η `netstat -i` πρέπει να αντικατασταθούν με άνω-κάτω τελείες, και κάθε μονό δεκαεξαδικό ψηφίο πρέπει να μετατραπεί σε διπλό προσθέτοντας από

μπροστά ένα μηδενικό. Η διεύθυνση μετατρέπεται με αυτό τον τρόπο σε μια μορφή που μπορεί να χρησιμοποιήσει η arp(8). Δείτε τη σελίδα manual της arp(8) για περισσότερες πληροφορίες σχετικά με τη χρήση της εντολής αυτής.

Όταν δημιουργείτε το /etc/sliphome/slip.login και το /etc/sliphome/slip.logout, θα πρέπει να θέσετε το bit "εκτέλεσης" (π.χ. `chmod 755 /etc/sliphome/slip.login /etc/sliphome/slip.logout`), διαφορετικά η `sliplogin` δεν θα μπορεί να τα εκτελέσει.

52.7.2.4.3. Ρύθμιση του slip.logout

Το /etc/sliphome/slip.logout δεν είναι απόλυτα απαραίτητο (εκτός αν πρόκειται να υλοποιήσετε "proxy ARP"), αλλά αν σκοπεύετε να το δημιουργήσετε, μπορείτε να χρησιμοποιήσετε ως υπόδειγμα το παρακάτω απλό παράδειγμα:

```
#!/bin/sh -
#
#       slip.logout

#
# logout file for a slip line.  sliplogin invokes this with
# the parameters:
#      1        2         3        4          5         6     7-n
#   slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 down
```

Αν χρησιμοποιείτε "proxy ARP", θα θέλετε το /etc/sliphome/slip.logout να διαγράφει την καταχώριση ARP του πελάτη SLIP:

```
#!/bin/sh -
#
#       @(#)slip.logout

#
# logout file for a slip line.  sliplogin invokes this with
# the parameters:
#      1        2         3        4          5         6     7-n
#   slipunit ttyspeed loginname local-addr remote-addr mask opt-args
#
/sbin/ifconfig sl$1 down
# Quit answering ARP requests for the SLIP client
/usr/sbin/arp -d $5
```

Η `arp -d $5` διαγράφει την καταχώριση ARP που προστέθηκε με την εκτέλεση του slip.login του "proxy ARP", κατά την είσοδο του πελάτη SLIP.

Πρέπει να το επαναλάβουμε άλλη μια φορά: Βεβαιωθείτε ότι το /etc/sliphome/slip.logout έχει οριστεί

ως εκτελέσιμο μετά την δημιουργία του (π.χ., `chmod 755 /etc/sliphome/slip.logout`).

52.7.2.5. Παράγοντες που Πρέπει να Λάβετε Υπόψη σας στη Δρομολόγηση

Αν δεν χρησιμοποιείτε την μέθοδο "proxy ARP" για να δρομολογείτε πακέτα μεταξύ των πελατών SLIP και του υπόλοιπου δικτύου σας (και ενδεχομένως και του Internet), θα πρέπει μάλλον να προσθέσετε στατικές διαδρομές προς τον πλησιέστερο σας προεπιλεγμένο δρομολογητή για να δρομολογείτε το υποδίκτυο των SLIP πελατών σας διαμέσου του εξυπηρετητή SLIP.

52.7.2.5.1. Στατικές Διαδρομές

Η προσθήκη στατικών διαδρομών προς τους πλησιέστερους σας προεπιλεγμένους δρομολογητές, μπορεί να είναι προβληματική (ή και αδύνατη αν δεν έχετε τα κατάλληλα δικαιώματα πρόσβασης). Αν η εταιρία σας διαθέτει δίκτυο με πολλαπλούς δρομολογητές, κάποια μοντέλα (π.χ. από την Cisco και την Proteon), εκτός ότι πρέπει να ρυθμιστούν με την στατική διαδρομή προς το υποδίκτυο SLIP, πρέπει επίσης να ρυθμιστούν με τις στατικές διαδρομές που θα αναφέρουν στους άλλους δρομολογητές. Θα χρειαστεί να πειραματιστείτε και να δοκιμάσετε διάφορες ρυθμίσεις για να δουλέψει η δρομολόγηση μέσω στατικών διαδρομών.

Chapter 53. Ηλεκτρονικό Ταχυδρομείο

53.1. Σύνοψη

Το "ηλεκτρονικό ταχυδρομείο", ευρύτερα γνωστό ως email, είναι στις μέρες μας μια από τις πλέον διαδεδομένες μορφές επικοινωνίας. Το κεφάλαιο αυτό παρέχει μια βασική εισαγωγή στη λειτουργία ενός διακομιστή email στο FreeBSD, καθώς και μια εισαγωγή στη διαδικασία αποστολής και λήψης email στο FreeBSD. Ωστόσο η αναφορά αυτή δεν πρέπει να θεωρηθεί πλήρης, καθώς υπάρχουν ακόμα αρκετοί παράγοντες που πρέπει να ληφθούν υπόψιν και έχουν εδώ παραλειφθεί. Για πιο πλήρη ανάλυση του θέματος, ο αναγνώστης παραπέμπεται στα πολλά εξαιρετικά βιβλία που αναφέρονται στο Βιβλιογραφία.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Το λογισμικό που χρησιμοποιείται στην αποστολή και λήψη ηλεκτρονικού ταχυδρομείου.
- Που βρίσκονται τα βασικά αρχεία ρυθμίσεων του sendmail στο FreeBSD.
- Τη διαφορά μεταξύ απομακρυσμένων και τοπικών θυρίδων ταχυδρομείου (mailboxes).
- Πως να εμποδίσετε ανεπιθύμητους spammers από το να χρησιμοποιήσουν τον δικό σας εξυπηρετητή email ως αναμεταδότη.
- Πως να εγκαταστήσετε και να ρυθμίσετε ένα εναλλακτικό Αντιπρόσωπο Μεταφοράς Ταχυδρομείου (Mail Transfer Agent) στο σύστημα σας, αντικαθιστώντας έτσι το sendmail.
- Πως να αντιμετωπίσετε συνηθισμένα προβλήματα στον διακομιστή ταχυδρομείου.
- Πως να χρησιμοποιήσετε το SMTP με το UUCP.
- Πως να ρυθμίσετε το σύστημα σας μόνο για αποστολή email.
- Πως να χρησιμοποιήσετε το email μέσω επιλογικής (dialup) σύνδεσης.
- Πως να ρυθμίσετε πιστοποίηση αυθεντικότητας στο SMTP για πρόσθετη ασφάλεια.
- Πως να εγκαταστήσετε και να χρησιμοποιήσετε μια εφαρμογή αποστολής και λήψης email για χρήστες, όπως το mutt.
- Πως να κατεβάσετε το email σας από ένα απομακρυσμένο διακομιστή POP ή IMAP.
- Πως να εφαρμόσετε φίλτρα και κανόνες στην εισερχόμενη αλληλογραφία σας, με αυτόματο τρόπο.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να ρυθμίσετε σωστά τη σύνδεση του δικτύου σας (Προχωρημένα Θέματα Δικτύωσης).
- Να ρυθμίσετε σωστά τις πληροφορίες DNS για τον διακομιστή αλληλογραφίας σας (Εξυπηρετητές Δικτύου).
- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

53.2. Χρησιμοποιώντας το Ηλεκτρονικό Ταχυδρομείο

Σε κάθε ανταλλαγή ηλεκτρονικού ταχυδρομείου, συνεργάζονται πέντε βασικά τμήματα: Το πρόγραμμα χρήστη, ο δαίμονας του εξυπηρετητή, το DNS, μια απομακρυσμένη ή τοπική θυρίδα ταχυδρομείου (mailbox) και φυσικά ο υπολογιστής που διαχειρίζεται το email (mailhost).

53.2.1. Το Πρόγραμμα Χρήστη

Η κατηγορία αυτή περιλαμβάνει προγράμματα όπως τα mutt, alpine, elm, και `mail`, καθώς και προγράμματα που διαθέτουν GUI όπως είναι τα balsa, xfmail (για να δώσουμε μερικά παραδείγματα) και κάποια πιο "εξελιγμένα" όπως είναι οι φυλλομετρητές για το WWW. Τα προγράμματα αυτά, απλώς μεταβιβάζουν τις συναλλαγές ταχυδρομείου στον τοπικό "mailhost", είτε καλώντας κάποιον από τους δαίμονες του εξυπηρετητή που είναι διαθέσιμοι, ή παραδίδοντας τις απευθείας μέσω TCP.

53.2.2. Δαίμονας Εξυπηρετητή Mailhost

Το FreeBSD έρχεται με το sendmail εγκατεστημένο από προεπιλογή, αλλά υποστηρίζει επίσης και μεγάλο αριθμό από άλλους δαίμονες ταχυδρομείου, περιλαμβανομένων και των:

- exim
- postfix
- qmail

Ο δαίμονας έχει συνήθως δύο λειτουργίες-είναι υπεύθυνος για τη λήψη εισερχόμενου mail, όπως επίσης και την παράδοση του εξερχόμενου mail. Όμως, *δεν είναι* υπεύθυνος για τη συλλογή του mail με τη χρήση πρωτοκόλλων όπως τα POP ή IMAP για την ανάγνωση του ταχυδρομείου σας, ούτε επιτρέπει τη σύνδεση στις τοπικές θυρίδες τύπου mbox ή Maildir. Πιθανόν να χρειαστείτε κάποιο επιπρόσθετο δαίμονα για αυτό το σκοπό.

Παλιότερες εκδόσεις του sendmail έχουν κάποια σοβαρά προβλήματα ασφαλείας, μέσω των οποίων μπορεί κάποιος εισβολέας να αποκτήσει τοπική ή απομακρυσμένη πρόσβαση στο μηχάνημα σας. Για να αποφύγετε προβλήματα τέτοιου είδους, βεβαιωθείτε ότι χρησιμοποιείτε κάποια πρόσφατη έκδοση. Εναλλακτικά, μπορείτε να εγκαταστήσετε κάποιο άλλο MTA από την Συλλογή των Ports του FreeBSD.

53.2.3. Email και DNS

Το Σύστημα Ονομασίας Περιοχών (DNS) και ο δαίμονας του, ο `named`, έχουν σημαντικό ρόλο στην παράδοση του email. Για την παράδοση του email από το ένα site σε ένα άλλο, ο δαίμονας του εξυπηρετητή θα ψάξει για το απομακρυσμένο site στο DNS, για να καθορίσει ποιος υπολογιστής λαμβάνει το email για το συγκεκριμένο προορισμό. Η διαδικασία αυτή συμβαίνει επίσης όταν ο δικός σας εξυπηρετητής λαμβάνει email από κάποιο απομακρυσμένο υπολογιστή.

Το DNS είναι υπεύθυνο για την αντιστοίχηση ονομάτων υπολογιστών σε διευθύνσεις IP, όπως και για την αποθήκευση πληροφοριών που σχετίζονται με την παράδοση ηλεκτρονικού ταχυδρομείου,

όπως οι εγγραφές MX. Η εγγραφή MX (Mail Exchanger) αναγνωρίζει ποιος υπολογιστής (ή υπολογιστές) θα είναι υπεύθυνος για τη λήψη ταχυδρομείου ενός συγκεκριμένου τομέα (domain). Αν δεν έχετε εγγραφή MX για τον υπολογιστή ή τον τομέα σας, το email θα παραδίδεται απευθείας στον υπολογιστή σας, με την προϋπόθεσή ότι έχετε εγγραφή τύπου A που να δείχνει στον υπολογιστή σας ή στην IP διεύθυνση του.

Μπορείτε να δείτε τις εγγραφές MX για οποιοδήποτε τομέα, χρησιμοποιώντας την εντολή host(1), όπως φαίνεται στο παρακάτω παράδειγμα:

```
% host -t mx FreeBSD.org
FreeBSD.org mail is handled (pri=10) by mx1.FreeBSD.org
```

53.2.4. Λαμβάνοντας Mail

Ο mailhost είναι υπεύθυνος για την λήψη mail που προορίζεται για τον τομέα σας. Θα συλλέξει όλο το mail που έρχεται προς τον τομέα, και θα το αποθηκεύσει είτε στο mbox (την προεπιλεγμένη μέθοδο για αποθήκευση mail) ή σε μορφή Maildir, ανάλογα με τις ρυθμίσεις που έχετε κάνει. Από τη στιγμή που το mail έχει αποθηκευθεί, μπορείτε είτε να το διαβάσετε τοπικά, χρησιμοποιώντας εφαρμογές όπως το mail(1) ή το mutt, ή να το δείτε μέσω απομακρυσμένης σύνδεσης, χρησιμοποιώντας κάποιο πρωτόκολλο όπως το POP ή το IMAP. Αυτό σημαίνει ότι αν επιθυμείτε να διαβάζετε το mail σας μόνο τοπικά, δεν χρειάζεται να εγκαταστήσετε εξυπηρετητή POP ή IMAP.

53.2.4.1. Πρόσβαση σε Απομακρυσμένες Θυρίδες μέσω POP και IMAP

Για να έχετε απομακρυσμένη πρόσβαση στις θυρίδες ταχυδρομείου, είναι απαραίτητο να έχετε πρόσβαση σε ένα εξυπηρετητή POP ή IMAP. Τα πρωτόκολλα αυτά, επιτρέπουν στους χρήστες να συνδέονται στις θυρίδες τους από απόσταση, με μεγάλη ευκολία. Και τα δύο πρωτόκολλα (POP και IMAP) επιτρέπουν στους χρήστες απομακρυσμένη πρόσβαση στις θυρίδες τους, αλλά το IMAP προσφέρει αρκετά πλεονεκτήματα, ορισμένα από τα οποία φαίνονται παρακάτω:

- Το IMAP μπορεί να αποθηκεύσει μηνύματα σε ένα απομακρυσμένο εξυπηρετητή, όπως επίσης και να τα ανακτήσει.
- Το IMAP υποστηρίζει ταυτόχρονες ενημερώσεις.
- Το IMAP μπορεί να φανεί εξαιρετικά χρήσιμο σε συνδέσεις χαμηλής ταχύτητας, καθώς επιτρέπει στους χρήστες να κατεβάσουν τη δομή των μηνυμάτων, χωρίς να κατεβάσουν το περιεχόμενο τους. Μπορεί επίσης να εκτελέσει εργασίες όπως εύρεση μηνυμάτων απευθείας στον εξυπηρετητή, ελαχιστοποιώντας με αυτό τον τρόπο τη μεταφορά δεδομένων μεταξύ των πελατών και των εξυπηρετητών.

Για να εγκαταστήσετε ένα εξυπηρετητή POP ή IMAP θα πρέπει να ακολουθήσετε τα επόμενα βήματα:

1. Επιλέξτε ένα εξυπηρετητή IMAP ή POP που να εξυπηρετεί τις ανάγκες σας. Οι παρακάτω εξυπηρετητές POP και IMAP είναι αρκετά διαδεδομένοι και αποτελούν καλά παραδείγματα:
   - qpopper
   - teapop

- imap-uw
- courier-imap
- dovecot

2. Εγκαταστήστε το δαίμονα POP ή IMAP της επιλογής σας, από την Συλλογή των Ports.
3. Αν χρειάζεται, τροποποιήστε το αρχείο /etc/inetd.conf για να φορτώσετε τον εξυπηρετητή POP ή IMAP.

Θα πρέπει να σημειώσουμε ότι τόσο το POP όσο και το IMAP μεταδίδουν πληροφορίες όπως το όνομα χρήστη και τον κωδικό σε μορφή απλού κειμένου. Αυτό σημαίνει ότι αν θέλετε να ασφαλίσετε τη μετάδοση πληροφοριών μέσω αυτών των πρωτοκόλλων, θα πρέπει να περάσετε αυτές τις συνδέσεις μέσω του ssh(1) (tunneling) ή να χρησιμοποιήσετε SSL. Η διαδικασία tunneling περιγράφεται με λεπτομέρεια στο SSH Tunneling και το SSL στο OpenSSL.

53.2.4.2. Πρόσβαση σε Τοπικές Θυρίδες Ταχυδρομείου

Μπορείτε να έχετε τοπική πρόσβαση στις θυρίδες ταχυδρομείου χρησιμοποιώντας απευθείας κάποιο πρόγραμμα αποστολής/λήψης (MUA) στον εξυπηρετητή που είναι αποθηκευμένες. Κατάλληλες εφαρμογές για αυτό το σκοπό είναι π.χ. το mutt ή το mail(1).

53.2.5. Ο Εξυπηρετητής Mail

Εξυπηρετητής mail θεωρείται ο υπολογιστής ο οποίος είναι υπεύθυνος για την παράδοση και λήψη mail για τον υπολογιστή σας, και ενδεχομένως για το δίκτυο σας.

53.3. Ρύθμιση του sendmail

Το sendmail(8) είναι ο προεπιλεγμένος Αντιπρόσωπος Μεταφοράς Ταχυδρομείου (Mail Transfer Agent, MTA) στο FreeBSD. Δουλειά του είναι να δέχεται το email από τους Αντιπροσώπους Email Χρήστη (Mail User Agents, MUA) και να το παραδίδει στο κατάλληλο mailer που ορίζεται στο αρχείο ρυθμίσεων του. Το sendmail μπορεί επίσης να δεχθεί συνδέσεις δικτύου και να παραδώσει το mail σε τοπικές θυρίδες ή και σε κάποιο άλλο πρόγραμμα.

Το sendmail χρησιμοποιεί τα ακόλουθα αρχεία ρυθμίσεων:

Όνομα Αρχείου	Λειτουργία
/etc/mail/access	Η βάση δεδομένων πρόσβασης του sendmail.
/etc/mail/aliases	Παρωνύμια (aliases) για τις θυρίδες (Mailboxes)
/etc/mail/local-host-names	Λίστα των υπολογιστών για τους οποίους το sendmail δέχεται mail
/etc/mail/mailer.conf	Ρυθμίσεις του προγράμματος mailer
/etc/mail/mailertable	Πίνακας παραδόσεων του mailer
/etc/mail/sendmail.cf	Το κεντρικό αρχείο ρυθμίσεων του sendmail

Όνομα Αρχείου	Λειτουργία
/etc/mail/virtusertable	Πίνακας εικονικών χρηστών και περιοχών (domains)

53.3.1. /etc/mail/access

Η βάση δεδομένων πρόσβασης καθορίζει ποιοι υπολογιστές ή διευθύνσεις IP έχουν πρόσβαση στον τοπικό εξυπηρετητή mail και τι είδους πρόσβαση έχουν. Η καταχώρηση ενός υπολογιστή μπορεί να έχει τις επιλογές `OK`, `REJECT`, `RELAY` ή απλά να μεταβιβάζει τον έλεγχο στη ρουτίνα διαχείρισης λαθών του sendmail με κάποιο συγκεκριμένο σφάλμα. Οι υπολογιστές που είναι καταχωρημένοι με την επιλογή `OK`, η οποία είναι και η προεπιλεγμένη, επιτρέπεται να στείλουν email σε αυτό τον υπολογιστή, εφόσον ο τελικός προορισμός του μηνύματος είναι το τοπικό μηχάνημα. Οι υπολογιστές που είναι καταχωρημένοι με την επιλογή `REJECT` απορρίπτονται για οποιαδήποτε επικοινωνία έχει να κάνει με μετάδοση mail. Οι υπολογιστές που είναι καταχωρημένοι με την επιλογή `RELAY`, έχουν τη δυνατότητα να στείλουν mail προς οποιαδήποτε κατεύθυνση μέσω του συγκεκριμένου εξυπηρετητή.

Παράδειγμα 21. Ρύθμιση της Βάσης Δεδομένων Πρόσβασης του sendmail

```
cyberspammer.com                550 We do not accept mail from spammers
FREE.STEALTH.MAILER@            550 We do not accept mail from spammers
another.source.of.spam          REJECT
okay.cyberspammer.com           OK
128.32                          RELAY
```

Σε αυτό το παράδειγμα έχουμε πέντε καταχωρήσεις. Οι διευθύνσεις που φαίνονται στην αριστερή πλευρά του πίνακα, επηρεάζονται από τη ενέργεια που φαίνεται στη δεξιά πλευρά. Τα πρώτα δύο παραδείγματα, επιστρέφουν ένα κωδικό σφάλματος στη ρουτίνα διαχείρισης λαθών του sendmail. Το μήνυμα εκτυπώνεται στον απομακρυσμένο υπολογιστή, όταν το mail που λαμβάνεται ανήκει σε κάποια από τις κατηγορίες της αριστερής πλευράς του πίνακα. Η επόμενη καταχώρηση απορρίπτει την παραλαβή mail από ένα συγκεκριμένο υπολογιστή στο Internet, τον `another.source.of.spam`. Η επόμενη καταχώρηση κάνει δεκτές τις συνδέσεις mail από τον υπολογιστή `okay.cyberspammer.com`, το όνομα του οποίου προσδιορίζεται ακριβέστερα σε σχέση με τη γραμμή `cyberspammer.com` που είδαμε παραπάνω. Γραμμές που καθορίζουν ονόματα με μεγαλύτερη ακρίβεια, έχουν προτεραιότητα σε σχέση με πιο ανακριβείς. Η τελευταία καταχώρηση επιτρέπει την αναμετάδοση (relaying) ηλεκτρονικού ταχυδρομείου από υπολογιστές με διευθύνσεις IP που ξεκινάνε με `128.32`. Οι υπολογιστές αυτοί, μπορούν να στείλουν mail μέσω του συγκεκριμένου εξυπηρετητή, το οποίο να κατευθύνεται σε άλλους εξυπηρετητές ταχυδρομείου.

Σε περίπτωση ανανέωσης αυτού του αρχείου, θα πρέπει να εκτελέσετε την εντολή `make` στον κατάλογο /etc/mail/ για να ανανεώσετε τη βάση δεδομένων.

53.3.2. /etc/mail/aliases

Η βάση δεδομένων των παρωνυμίων (aliases), περιέχει μια λίστα από εικονικές θυρίδες ταχυδρομείου που επεκτείνονται σε άλλους χρήστες, αρχεία ή και άλλα παρωνύμια. Μερικά

παραδείγματα χρήσης του /etc/mail/aliases φαίνονται παρακάτω:

Παράδειγμα 22. Παρωνύμια Mail

```
root: localuser
ftp-bugs: joe,eric,paul
bit.bucket:  /dev/null
procmail: "|/usr/local/bin/procmail"
```

Η μορφή του αρχείου είναι απλή. Το όνομα της θυρίδας βρίσκεται στην αριστερή πλευρά της άνω-κάτω τελείας, και επεκτείνεται στον προορισμό που βρίσκεται στη δεξιά πλευρά. Το πρώτο παράδειγμα, ορίζει ότι η θυρίδα του χρήστη `root` θα είναι στην πραγματικότητα η θυρίδα `localuser`. Για την θυρίδα αυτή, γίνεται ξανά αναζήτηση στη βάση δεδομένων των παρωνυμιών. Αν δεν βρεθεί άλλο όνομα που να ταιριάζει, το μήνυμα θα παραδοθεί στον τοπικό χρήστη `localuser`. Το επόμενο παράδειγμα δείχνει μια λίστα ταχυδρομείου. Τα μηνύματα που απευθύνονται στη θυρίδα `ftp-bugs`, κατευθύνονται σε τρεις τοπικές θυρίδες, τις `joe`, `eric` και `paul`. Σημειώστε ότι είναι δυνατόν να καθοριστεί μια απομακρυσμένη θυρίδα χρησιμοποιώντας τη μορφή user@example.com. Το επόμενο παράδειγμα, δείχνει πως μπορεί να γίνει εγγραφή του mail σε ένα αρχείο, στη συγκεκριμένη περίπτωση το /dev/null. Το τελευταίο παράδειγμα, δείχνει πως γίνεται η αποστολή mail προς ένα πρόγραμμα. Στο παράδειγμα αυτό, το μήνυμα γράφεται στην τυποποιημένη είσοδο (standard input) του προγράμματος /usr/local/bin/procmail χρησιμοποιώντας ένα UNIX® pipe.

Κάθε φορά που γίνεται ενημέρωση αυτού του αρχείου, θα πρέπει να εκτελείτε την εντολή `make` στον κατάλογο /etc/mail/, ώστε να ενημερωθεί η βάση δεδομένων.

53.3.3. /etc/mail/local-host-names

Πρόκειται για μια λίστα από ονόματα υπολογιστών, την οποία το sendmail(8) θα δέχεται ως ονόματα για το τοπικό μηχάνημα. Τοποθετήστε σε αυτήν τα ονόματα των υπολογιστών ή των τομέων για τους οποίους θέλετε το sendmail να λαμβάνει mail. Για παράδειγμα, αν ο συγκεκριμένος εξυπηρετητής mail πρόκειται να λαμβάνει mail για τον τομέα `example.com` και για τον υπολογιστή `mail.example.com`, το αρχείο local-host-names θα μοιάζει με το παρακάτω:

```
example.com
mail.example.com
```

Κάθε φορά που ενημερώνεται αυτό το αρχείο, θα πρέπει να γίνεται επανεκκίνηση του sendmail(8) για να διαβάσει τις αλλαγές.

53.3.4. /etc/mail/sendmail.cf

Το sendmail.cf είναι το κεντρικό αρχείο ρυθμίσεων του sendmail. Το αρχείο αυτό ρυθμίζει τη συνολική συμπεριφορά του sendmail, που περιλαμβάνει μεταξύ άλλων την επανεγγραφή διευθύνσεων και την αποστολή μηνυμάτων απόρριψης προς απομακρυσμένους εξυπηρετητές mail. Καθώς το αρχείο αυτό περιέχει τόσο διαφορετικές ρυθμίσεις, είναι φυσικό να είναι αρκετά πολύπλοκο και οι λεπτομέρειες του είναι έξω από το σκοπό αυτής της ενότητας. Ευτυχώς, αυτό το

αρχείο σπάνια χρειάζεται να αλλαχθεί σε τυπικούς εξυπηρετητές mail.

Το βασικό αρχείο ρυθμίσεων του sendmail μπορεί να παραχθεί με τη βοήθεια μακροεντολών τύπου m4(1) που καθορίζουν τη συμπεριφορά και τα χαρακτηριστικά του sendmail. Για περισσότερες πληροφορίες, παρακαλούμε διαβάστε το /usr/src/contrib/sendmail/cf/README.

Για να ισχύσουν οι αλλαγές που κάνετε σε αυτό το αρχείο, θα πρέπει να επανεκκινήσετε το sendmail.

53.3.5. /etc/mail/virtusertable

Το αρχείο virtusertable αντιστοιχεί διευθύνσεις mail εικονικών τομέων σε πραγματικές θυρίδες ταχυδρομείου. Οι θυρίδες αυτές μπορεί να είναι τοπικές, απομακρυσμένες, παρωνύμια που έχουν οριστεί στο /etc/mail/aliases, ή αρχεία.

Παράδειγμα 23. Παράδειγμα Αντιστοίχησης Mail Εικονικού Τομέα

```
root@example.com                root
postmaster@example.com          postmaster@noc.example.net
@example.com                    joe
```

Στο παραπάνω παράδειγμα, έχουμε μια αντιστοίχηση για τον τομέα `example.com`. Η επεξεργασία αυτού του αρχείου γίνεται από πάνω προς τα κάτω, και σταματάει στην εύρεση του πρώτου ονόματος που ταιριάζει. Η πρώτη γραμμή του παραδείγματος, αντιστοιχεί το root@example.com στην τοπική θυρίδα `root`. Η επόμενη καταχώρηση αντιστοιχεί το postmaster@example.com στη θυρίδα `postmaster` στον υπολογιστή `noc.example.net`. Τέλος, αν δεν βρεθεί καμιά αντιστοίχηση για τον τομέα `example.com`, θα εφαρμοστεί η τελευταία αντιστοίχηση, η οποία ταιριάζει με οποιοδήποτε mail σταλθεί προς τον τομέα `example.com`. Στην περίπτωση αυτή, το μήνυμα θα παραδοθεί στην τοπική θυρίδα `joe`.

53.4. Αλλάζοντας τον Αντιπρόσωπο Μεταφοράς Ταχυδρομείου (MTA)

Όπως έχουμε ήδη αναφέρει, το FreeBSD έρχεται με το sendmail προεγκατεστημένο ως Αντιπρόσωπο Μεταφοράς Ταχυδρομείου (Mail Transfer Agent, MTA). Το πρόγραμμα αυτό είναι από προεπιλογή υπεύθυνο για την εισερχόμενη και εξερχόμενη αλληλογραφία.

Υπάρχει ωστόσο πληθώρα λόγων για τους οποίους κάποιοι διαχειριστές επιλέγουν να αλλάξουν το MTA του συστήματος τους. Οι λόγοι αυτοί κυμαίνονται από το ότι απλά θέλουν να δοκιμάσουν κάποιο άλλο MTA, ως και το ότι χρειάζονται κάποιο ιδιαίτερο χαρακτηριστικό ή δυνατότητα που υπάρχει σε κάποιο άλλο mailer. Ευτυχώς, το FreeBSD κάνει εύκολη την αλλαγή του αντιπροσώπου.

53.4.1. Εγκαταστήστε Νέο MTA

Υπάρχουν αρκετοί MTA για να επιλέξετε. Ένα καλό σημείο εκκίνησης είναι η Συλλογή των Ports του FreeBSD όπου και θα μπορέσετε να βρείτε αρκετούς. Φυσικά είστε ελεύθερος να επιλέξετε όποιο

MTA θέλετε από οπουδήποτε, όσο τουλάχιστον μπορείτε να το κάνετε να εκτελείτε στο FreeBSD.

Ξεκινήστε εγκαθιστώντας το νέο σας MTA. Μετά την εγκατάσταση, θα έχετε την ευκαιρία να αποφασίσετε αν πραγματικά καλύπτει τις ανάγκες σας, καθώς και να ολοκληρώσετε τις ρυθμίσεις του πριν μεταφέρετε τη διαχείριση mail του συστήματος από το sendmail στο νέο σας πρόγραμμα. Κατά την εγκατάσταση, βεβαιωθείτε ότι το νέο σας λογισμικό δεν θα προσπαθήσει να εγκατασταθεί πάνω στα υπάρχοντα εκτελέσιμα του συστήματος, όπως το /usr/bin/sendmail. Διαφορετικά, θα έχετε ουσιαστικά βάλει το νέο σας λογισμικό mail σε χρήση, πριν προλάβετε καλά-καλά να το ρυθμίσετε.

Παρακαλούμε να διαβάσετε την τεκμηρίωση του MTA που επιλέξατε, για πληροφορίες σχετικά με τη ρύθμιση του.

53.4.2. Απενεργοποιήστε το sendmail

Αν απενεργοποιήσετε τη δυνατότητα αποστολής (εξερχόμενα) του sendmail, είναι σημαντικό να την αντικαταστήσετε με ένα εναλλακτικό σύστημα παράδοσης mail. Αν επιλέξετε να μην κάνετε το παραπάνω, τα μηνύματα του συστήματος, όπως αυτά που παράγονται από το periodic(8), δεν θα μπορούν να παραδοθούν μέσω email, όπως είναι το αναμενόμενο. Πολλά τμήματα του συστήματος σας αναμένουν ότι υπάρχει σε λειτουργία ένα σύστημα συμβατό με το sendmail. Αν οι εφαρμογές συνεχίζουν να χρησιμοποιούν τα εκτελέσιμα του sendmail προσπαθώντας να στείλουν email μετά την απενεργοποίηση του, το mail πιθανώς θα βρεθεί σε μια ανενεργή ουρά του sendmail και δεν θα παραδοθεί ποτέ.

Για να απενεργοποιήσετε εντελώς το sendmail, συμπεριλαμβανομένης και της υπηρεσίας εξερχόμενων μηνυμάτων, χρησιμοποιήστε:

```
sendmail_enable="NO"
sendmail_submit_enable="NO"
sendmail_outbound_enable="NO"
sendmail_msp_queue_enable="NO"
```

στο /etc/rc.conf.

Αν θέλετε να απενεργοποιήσετε μόνο την υπηρεσία εισερχομένων του sendmail θα πρέπει να θέσετε:

```
sendmail_enable="NO"
```

στο /etc/rc.conf. Περισσότερες πληροφορίες για τις επιλογές εκκίνησης του sendmail, διατίθενται από την αντίστοιχη σελίδα manual, rc.sendmail(8).

53.4.3. Εκκίνηση του Νέου σας MTA κατά την Εκκίνηση

Το νέο σας MTA θα ξεκινάει κατά την εκκίνηση, αν προσθέσετε μια κατάλληλη γραμμή στο αρχείο /etc/rc.conf. Δείτε το παρακάτω παράδειγμα για το postfix:

```
# echo 'postfix_enable="YES"' >> /etc/rc.conf
```

Το MTA θα ξεκινάει πλέον κατά την εκκίνηση.

53.4.4. Αντικαθιστώντας το sendmail από Προεπιλεγμένο Mailer Συστήματος

Το sendmail είναι τόσο γνωστό ως στάνταρ λογισμικό στα συστήματα UNIX®, ώστε πολλά άλλα προγράμματα θεωρούν ότι είναι ήδη εγκατεστημένο και ρυθμισμένο. Για το λόγο αυτό, πολλά εναλλακτικά MTA παρέχουν δικές τους συμβατές υλοποιήσεις του sendmail. Οι υλοποιήσεις αυτές παρέχουν παρόμοιο σύνολο εντολών, και μπορούν έτσι να χρησιμοποιηθούν ώστε να αντικαταστήσουν "απευθείας" το sendmail.

Για το λόγο αυτό, αν χρησιμοποιείτε κάποιο εναλλακτικό mailer, θα θέλετε να εξασφαλίσετε ότι άλλα προγράμματα που προσπαθούν να εκτελέσουν τα τυπικά εκτελέσιμα του sendmail όπως το /usr/bin/sendmail, θα εκτελέσουν στην πραγματικότητα τον επιλεγμένο σας mailer. Ευτυχώς, το FreeBSD παρέχει ένα σύστημα που καλείτε mailwrapper(8) και το οποίο αναλαμβάνει αυτή τη δουλειά για σας.

Όταν το sendmail λειτουργεί όπως έχει εγκατασταθεί αρχικά, θα βρείτε κάτι όπως το παρακάτω στο /etc/mail/mailer.conf:

```
sendmail     /usr/libexec/sendmail/sendmail
send-mail   /usr/libexec/sendmail/sendmail
mailq       /usr/libexec/sendmail/sendmail
newaliases  /usr/libexec/sendmail/sendmail
hoststat    /usr/libexec/sendmail/sendmail
purgestat   /usr/libexec/sendmail/sendmail
```

Αυτό σημαίνει ότι όταν εκτελείται κάποια από αυτές τις συνηθισμένες εντολές (όπως το ίδιο το sendmail), το σύστημα στην πραγματικότητα εκτελεί ένα αντίγραφο του mailwrapper που ονομάζεται sendmail, και το οποίο ελέγχει το mailer.conf και εκτελεί το /usr/libexec/sendmail/sendmail αντί αυτού. Το σύστημα αυτό διευκολύνει ιδιαίτερα την αλλαγή των εκτελέσιμων που εκτελούνται στην πραγματικότητα όταν γίνεται κλήση των προεπιλεγμένων λειτουργιών του sendmail.

Έτσι, αν θέλετε να εκτελείται το /usr/local/supermailer/bin/sendmail-compat αντί για το sendmail, θα μπορούσατε να αλλάξετε το /etc/mail/mailer.conf ώστε να γράφει:

```
sendmail     /usr/local/supermailer/bin/sendmail-compat
send-mail   /usr/local/supermailer/bin/sendmail-compat
mailq       /usr/local/supermailer/bin/mailq-compat
newaliases  /usr/local/supermailer/bin/newaliases-compat
hoststat    /usr/local/supermailer/bin/hoststat-compat
purgestat   /usr/local/supermailer/bin/purgestat-compat
```

53.4.5. Ολοκληρώνοντας

Μόλις έχετε ρυθμίσει τα πάντα όπως επιθυμείτε, μπορείτε είτε να κάνετε kill τις διεργασίες του sendmail που δεν χρειάζεστε πλέον και να εκκινήσετε τις αντίστοιχες του νέου σας λογισμικού, ή απλώς να κάνετε επανεκκίνηση. Η επανεκκίνηση θα σας δώσει επίσης την ευκαιρία να βεβαιωθείτε ότι το σύστημα σας έχει ρυθμιστεί σωστά, ώστε το νέο σας MTA να ξεκινάει αυτόματα σε κάθε εκκίνηση.

53.5. Αντιμετώπιση Προβλημάτων

53.5.1. Γιατί πρέπει να χρησιμοποιώ το πλήρες όνομα (FQDN) για υπολογιστές που βρίσκονται στον τομέα μου;

Το πιο πιθανό είναι να διαπιστώσετε ότι ο υπολογιστής βρίσκεται στην πραγματικότητα σε διαφορετικό τομέα. Για παράδειγμα, αν βρίσκεστε στο `foo.bar.edu` και θέλετε να επικοινωνήσετε με ένα υπολογιστή με το όνομα `mumble` στον τομέα `bar.edu`, θα πρέπει να αναφερθείτε σε αυτόν με το πλήρες του όνομα, `mumble.bar.edu`, αντί για απλώς `mumble`.

Παραδοσιακά, αυτό επιτρεπόταν από τους DNS resolvers του BIND. Ωστόσο, η τρέχουσα έκδοση του BIND που περιλαμβάνεται στο FreeBSD, δεν παρέχει πλέον συντομεύσεις για μη-πλήρη ονόματα τομέων, εκτός για τον τομέα στον οποίο βρίσκεστε. Έτσι, ένας υπολογιστής με μη-πλήρες όνομα `mumble` θα πρέπει να βρεθεί ως `mumble.foo.bar.edu`, ή θα γίνει αναζήτηση για αυτόν στο ριζικό τομέα.

Η συμπεριφορά αυτή είναι διαφορετική από την προηγούμενη, όπου η αναζήτηση συνεχιζόταν και στο `mumble.bar.edu`, και το `mumble.edu`. Ρίξτε μια ματιά στο RFC 1535 για το λόγο που το παραπάνω θεωρείτε κακή πρακτική, ή ακόμα και κενό ασφαλείας.

Ένας τρόπος για να παρακάμψετε το πρόβλημα είναι να προσθέσετε τη γραμμή:

```
search foo.bar.edu bar.edu
```

αντί για την προηγούμενη:

```
domain foo.bar.edu
```

στο αρχείο /etc/resolv.conf. Βεβαιωθείτε ωστόσο ότι η σειρά αναζήτησης δεν πηγαίνει πέρα από το "όριο μεταξύ τοπικής και δημόσιας διαχείρισης", όπως το αποκαλεί το RFC 1535.

53.5.2. Το sendmail δίνει το μήνυμα mail loops back to myself (το mail επιστρέφει στον εαυτό μου)

Η απάντηση σε αυτό, υπάρχει στο FAQ του sendmail όπως φαίνεται παρακάτω:

```
Λαμβάνω αυτά τα μηνύματα λάθους:

553 MX list for domain.net points back to relay.domain.net
```

```
554 <user@domain.net>... Local configuration error

Πως μπορώ να λύσω το πρόβλημα;

Έχετε ζητήσει το mail προς ένα τομέα (π.χ. το domain.net) να
προωθείται προς ένα συγκεκριμένο υπολογιστή (στην περίπτωση αυτή
το relay.domain.net) χρησιμοποιώντας μια εγγραφή
MXMX record, αλλά το
μηχάνημα αναμετάδοσης (relay) δεν αναγνωρίζει τον εαυτό του ως
domain.net.  Προσθέστε το domain.net στο /etc/mail/local-host-names
[είναι γνωστό ως /etc/sendmail.cw πριν την έκδοση 8.10]
(αν χρησιμοποιείτε το FEATURE(use_cw_file)), διαφορετικά προσθέστε το
Cw domain.net στο /etc/mail/sendmail.cf.
```

Μπορείτε να βρείτε το FAQ του sendmail στη διεύθυνση http://www.sendmail.org/faq/, και συνίσταται να το διαβάσετε αν θέλετε να "πειράξετε" τις ρυθμίσεις του mail σας.

53.5.3. Πως μπορώ να εκτελέσω εξυπηρετητή mail σε υπολογιστή που συνδέεται μέσω επιλογικής σύνδεσης PPP;

Θέλετε να συνδέσετε ένα FreeBSD μηχάνημα σε ένα τοπικό δίκτυο (LAN) στο Internet. Το FreeBSD μηχάνημα θα γίνει πύλη ταχυδρομείου για το LAN. Η σύνδεση PPP δεν είναι αποκλειστική.

Υπάρχουν τουλάχιστον δύο τρόποι για να το κάνετε αυτό. Ο ένας είναι με τη χρήση UUCP.

Ένας άλλος τρόπος είναι να βάλετε ένα εξυπηρετητή Internet ο οποίος έχει συνεχή σύνδεση, να σας παρέχει υπηρεσία δευτερεύοντος MX για τον τομέα σας. Για παράδειγμα, αν ο τομέας της εταιρίας σας είναι `example.com` και ο παροχέας σας Internet έχει ορίσει το `example.net` να παρέχει υπηρεσίες δευτερεύοντος MX για τον τομέα σας:

```
example.com.          MX        10      example.com.
                      MX        20      example.net.
```

Μόνο ένας υπολογιστής μπορεί να καθοριστεί ως τελικός παραλήπτης (προσθέστε το `Cw example.com` στο αρχείο /etc/mail/sendmail.cf στο `example.com`).

Όταν το μηχάνημα που στέλνει μέσω του `sendmail` προσπαθεί να παραδώσει το mail θα προσπαθήσει να συνδεθεί στο δικό σας (`example.com`) μέσω της σύνδεσης modem. Το πιο πιθανό είναι ότι δεν θα τα καταφέρει, γιατί δεν θα είστε συνδεμένος εκείνη τη στιγμή. Το sendmail θα το παραδώσει αυτόματα στην υπηρεσία δευτερεύοντος MX, π.χ. τον παροχέα σας Internet (`example.net`). Το δευτερεύον MX θα προσπαθεί περιοδικά να συνδεθεί στο μηχάνημα σας και να παραδώσει το mail στον κύριο εξυπηρετητή MX (`example.com`).

Μπορείτε να χρησιμοποιήσετε κάτι όπως το παρακάτω ως script εισόδου:

```
#!/bin/sh
# Put me in /usr/local/bin/pppmyisp
( sleep 60 ; /usr/sbin/sendmail -q ) &
```

```
/usr/sbin/ppp -direct pppmyisp
```

Αν πρόκειται να χρησιμοποιήσετε χωριστό script για την είσοδο κάποιου χρήστη, μπορείτε να χρησιμοποιήσετε αντί για το παραπάνω το `sendmail -qRexample.com` στο script. Αυτό θα εξαναγκάσει την άμεση επεξεργασία όλου του mail στην ουρά για το `example.com`.

Πιο λεπτομερής περιγραφή της κατάστασης φαίνεται παρακάτω:

Μήνυμα από την ηλεκτρονική λίστα του FreeBSD για τους παροχείς υπηρεσιών Internet.

```
> παρέχουμε δευτερεύον MX για ένα πελάτη.  Ο πελάτης συνδέεται στις
> υπηρεσίες μας αρκετές φορές τη μέρα αυτόματα, για να λαμβάνει τα email του
> στο πρωτεύον του MX (Δεν καλούμε την τοποθεσία του όταν λαμβάνουμε email
> για τον τομέα του).  Το sendmail μας στέλνει το  mailqueue κάθε 30 λεπτά.
> Τη δεδομένη στιγμή θα πρέπει να μείνει συνδεμένος για 30 λεπτά,
> για να είναι βέβαιος ότι όλο το email του θα έχει
> παραδοθεί στον πρωτεύοντα MX.
>
> Υπάρχει κάποια εντολή που να εξαναγκάσει το sendmail να στείλει
> όλα τα mails άμεσα; Ο χρήστης φυσικά δεν έχει δικαιώματα
> root στο μηχάνημα μας.

Στην ενότητα privacy flags του sendmail.cf, υπάρχει ένας
ορισμός Opgoaway,restrictqrun

Αφαιρέστε το restrictqrun για να επιτρέψετε σε μη-root χρήστες να ξεκινήσουν
την επεξεργασία της ουράς.
Μπορεί επίσης να θέλετε να αναδιατάξετε τα MX.  Είμαστε το 1ο MX για αυτού
του είδους τους πελάτες, και έχουμε ορίσει:

# If we are the best MX for a host, try directly instead of generating
# local config error.
OwTrue

Με τον τρόπο αυτό, ένα απομακρυσμένο site θα παραδίδει απευθείας σε σας,
χωρίς να προσπαθεί τη σύνδεση με το χρήστη.  Έπειτα τα στέλνετε στον
πελάτη σας.  Αυτό λειτουργεί μόνο για μηχανήματα, και έτσι
χρειάζεται να βάλετε τον πελάτη σας να ονομάσει το μηχάνημα του mail
customer.com και επίσης
hostname.customer.com στο DNS.  Απλώς προσθέστε μια εγγραφή
τύπου A στο DNS για το customer.com.
```

53.5.4. Γιατί λαμβάνω συνέχεια μηνύματα λάθους Relaying Denied όταν στέλνω mail από άλλους υπολογιστές;

Στις προεπιλεγμένες εγκαταστάσεις του FreeBSD, το sendmail είναι ρυθμισμένο να στέλνει mail μόνο από τον υπολογιστή στον οποίο εκτελείται. Για παράδειγμα, αν υπάρχει διαθέσιμος διακομιστής POP, οι χρήστες θα μπορούν να ελέγχουν το mail τους από το σχολείο, το γραφείο, ή άλλη απομακρυσμένη τοποθεσία, αλλά θα εξακολουθούν να μην μπορούν να στείλουν προς

εξωτερικές διευθύνσεις. Τυπικά, λίγο μετά από μια απόπειρα αποστολής, θα σταλεί ένα email από τον MAILER-DAEMON με το μήνυμα λάθους `5.7 Relaying Denied`.

Υπάρχουν διάφοροι τρόποι για να ξεπεράσετε το πρόβλημα. Ο πλέον απλός είναι να βάλετε τη διεύθυνση του ISP σας σε ένα αρχείο relay-domains, /etc/mail/relay-domains. Ένας γρήγορος τρόπος για να το κάνετε αυτό είναι:

```
# echo "your.isp.example.com" > /etc/mail/relay-domains
```

Αφού δημιουργήσετε ή επεξεργαστείτε αυτό το αρχείο, θα πρέπει να επανεκκινήσετε το sendmail. Αυτό δουλεύει μια χαρά αν είστε διαχειριστής εξυπηρετητή και δεν επιθυμείτε να στέλνετε mail τοπικά, ή αν θέλετε να χρησιμοποιήσετε ένα σύστημα τύπου point και click σε ένα άλλο μηχάνημα ή ακόμα και σε άλλο ISP. Είναι επίσης πολύ χρήσιμο αν έχετε ρυθμίσει μόνο ένα ή δύο λογαριασμούς mail. Αν θέλετε να προσθέσετε μεγαλύτερο αριθμό διευθύνσεων, μπορείτε να ανοίξετε αυτό το αρχείο με τον επιθυμητό συντάκτη κειμένου, και να προσθέσετε όλους τους τομείς, ένα σε κάθε γραμμή:

```
your.isp.example.com
other.isp.example.net
users-isp.example.org
www.example.org
```

Τώρα, οποιαδήποτε αποστολή mail από το σύστημα σας από οποιοδήποτε υπολογιστή αυτής της λίστας (με την προϋπόθεσή ο χρήστης να έχει λογαριασμό στο σύστημα σας), θα είναι επιτυχής. Πρόκειται για ένα πολύ καλό τρόπο να επιτρέψετε στους χρήστες να στέλνουν mail από το σύστημα σας μέσω απομακρυσμένης σύνδεσης, χωρίς να επιτρέπετε σε άλλους να στέλνουν SPAM μέσω του συστήματος σας.

53.6. Προχωρημένα Θέματα

Η ακόλουθη ενότητα καλύπτει πιο προχωρημένα θέματα, όπως τη ρύθμιση του mail και ρυθμίσεις για ένα ολόκληρο τομέα.

53.6.1. Βασικές Ρυθμίσεις

Χωρίς να χρειαστεί να κάνετε καμιά ρύθμιση, θα μπορείτε να στείλετε mail προς εξωτερικούς υπολογιστές, αρκεί να έχετε ρυθμίσει το /etc/resolv.conf ή να εκτελείτε το δικό σας εξυπηρετητή DNS. Αν θέλετε να παραλαμβάνετε mail για τον υπολογιστή σας στο δικό σας sendmail MTA, υπάρχουν δύο μέθοδοι:

- Μπορείτε να έχετε δικό σας τομέα και δικό σας εξυπηρετητή DNS για τον τομέα σας. Για παράδειγμα, `FreeBSD.org`
- Να παραλαμβάνετε mail απευθείας στο μηχάνημα σας. Αυτό γίνεται αν το mail παραδίδεται απευθείας στον υπολογιστή σας, χρησιμοποιώντας τον όνομα του (πρέπει να βρίσκεται στο DNS). Για παράδειγμα, `example.FreeBSD.org`.

Όποια επιλογή από τις παραπάνω και να κάνατε, για να είναι δυνατή η παραλαβή mail απευθείας στον υπολογιστή σας, θα πρέπει να έχετε μόνιμη στατική διεύθυνση IP (όχι δυναμική, όπως είναι οι περισσότερες επιλογικές συνδέσεις PPP). Αν βρίσκεστε πίσω από κάποιο firewall, θα πρέπει να επιτρέπει τη διακίνηση SMTP προς εσάς. Αν θέλετε να λαμβάνετε mail απευθείας στον υπολογιστή σας, θα πρέπει να εξασφαλίσετε *ένα* από τα παρακάτω:

- Να βεβαιωθείτε ότι η εγγραφή MX (με το χαμηλότερο αριθμό) στο DNS σας, δείχνει προς τη διεύθυνση IP του μηχανήματος σας.
- Να βεβαιωθείτε ότι δεν υπάρχει καμιά εγγραφή MX στο DNS για τον υπολογιστή σας.

Όποιο από τα παραπάνω και αν κάνετε, θα μπορείτε να λαμβάνετε mail απευθείας στον υπολογιστή σας.

Δοκιμάστε αυτό:

```
# hostname
example.FreeBSD.org
# host example.FreeBSD.org
example.FreeBSD.org has address 204.216.27.XX
```

Αν βλέπετε το παραπάνω, το mail που κατευθύνεται απευθείας στο yourlogin@example.FreeBSD.org θα πρέπει να λαμβάνεται χωρίς προβλήματα (θεωρώντας ότι το sendmail εκτελείτε σωστά στον υπολογιστή `example.FreeBSD.org`).

Αν αντί για αυτό δείτε κάτι σαν το παρακάτω:

```
# host example.FreeBSD.org
example.FreeBSD.org has address 204.216.27.XX
example.FreeBSD.org mail is handled (pri=10) by hub.FreeBSD.org
```

Όλο το mail που κατευθύνεται προς τον υπολογιστή σας (`example.FreeBSD.org`) θα καταλήξει να συλλέγεται στο `hub` με το ίδιο όνομα χρήστη, αντί να σταλεί απευθείας στο μηχάνημα σας.

Τις παραπάνω πληροφορίες, τις χειρίζεται ο δικός σας εξυπηρετητής DNS. Η εγγραφή DNS που περιέχει τις πληροφορίες δρομολόγησης για το mail, είναι η *M*ail e*X*change. Αν δεν υπάρχει εγγραφή MX, το mail θα παραδίδεται απευθείας στον υπολογιστή μέσω της IP διεύθυνσης του.

Η καταχώριση MX για τον `freefall.FreeBSD.org` έμοιαζε κάποια στιγμή με την παρακάτω:

```
freefall        MX   30   mail.crl.net
freefall        MX   40   agora.rdrop.com
freefall        MX   10   freefall.FreeBSD.org
freefall        MX   20   who.cdrom.com
```

Όπως μπορείτε να δείτε, ο `freefall` είχε πολλές καταχωρήσεις MX. Η καταχώρηση με τον μικρότερο αριθμό, είναι ο υπολογιστής που λαμβάνει το mail απευθείας, αν είναι διαθέσιμος. Αν για κάποιο λόγο δεν είναι προσβάσιμος, οι άλλοι (που ορισμένες φορές καλούνται "backup MXes") δέχονται τα

μηνύματα προσωρινά και τα μεταβιβάζουν σε κάποιο υπολογιστή με χαμηλότερη αρίθμηση, μόλις γίνει διαθέσιμος. Τελικά τα μηνύματα καταλήγουν στον υπολογιστή με το μικρότερο αριθμό.

Οι εναλλακτικές τοποθεσίες MX, θα πρέπει να χρησιμοποιούν διαφορετικές γραμμές για τη σύνδεση τους με το Internet. Αυτή είναι η καλύτερη λύση. Ο παροχέας σας ή κάποιο άλλο φιλικό site, δεν θα έχουν κανένα πρόβλημα να σας παρέχουν αυτή την υπηρεσία.

53.6.2. Mail για τον Τομέα Σας

Για να δημιουργήσετε ένα "mailhost" (δηλ. ένα εξυπηρετητή mail) θα πρέπει οποιοδήποτε mail στέλνεται προς κάποιο σταθμό εργασίας, να λαμβάνεται σε αυτόν. Βασικά θα θέλετε να "διεκδικείτε" οποιοδήποτε mail που κατευθύνεται προς οποιοδήποτε όνομα μηχανήματος του τομέα σας (στην περίπτωση μας το `*.FreeBSD.org`) και να το ανακατευθύνετε προς τον εξυπηρετητή mail, ώστε οι χρήστες σας να μπορούν να λάβουν το mail τους από τον κεντρικό εξυπηρετητή.

Για ευκολία, θα πρέπει να έχετε ένα λογαριασμό χρήστη με το ίδιο *όνομα χρήστη* και στα δύο μηχανήματα. Χρησιμοποιήστε για το σκοπό αυτό την εντολή adduser(8).

Ο mailhost που θα χρησιμοποιήσετε, πρέπει να είναι το καθορισμένο μηχάνημα για την ανταλλαγή μηνυμάτων για κάθε σταθμό εργασίας του δικτύου. Αυτό γίνεται στις ρυθμίσεις DNS με τον ακόλουθο τρόπο:

```
example.FreeBSD.org        A      204.216.27.XX     ; Workstation
                           MX  10 hub.FreeBSD.org      ; Mailhost
```

Με τον τρόπο αυτό, το mail που κατευθύνεται προς κάποιο σταθμό εργασίας θα ανακατευθυνθεί προς το mailhost, άσχετα με το που δείχνει η εγγραφή τύπου A. Το mail στέλνεται προς τον υπολογιστή MX.

Δεν μπορείτε να κάνετε το παραπάνω, αν δεν εκτελείτε το δικό σας εξυπηρετητή DNS. Αν αυτό δεν συμβαίνει, και δεν μπορείτε να το αλλάξετε, συνεννοηθείτε με τον παροχέα σας (ISP) ή με όποιον σας παρέχει υπηρεσίες DNS.

Αν παρέχετε υπηρεσίες εικονικού ταχυδρομείου, οι παρακάτω πληροφορίες θα σας φανούν χρήσιμες. Για το παράδειγμα μας, θα υποθέσουμε ότι έχετε ένα πελάτη με το δικό του τομέα, στην περίπτωση μας το `customer1.org`, και θέλετε όλο το mail για το `customer1.org` να στέλνεται στο δικό σας mailhost, `mail.myhost.com`. Η καταχώριση σας στο DNS θα μοιάζει με την παρακάτω:

```
customer1.org       MX  10  mail.myhost.com
```

Σημειώστε ότι *δεν χρειάζεστε* εγγραφή τύπου A για το `customer1.org` αν θέλετε απλώς να χειρίζεστε email για αυτό τον τομέα.

Να έχετε υπόψη σας ότι δεν θα μπορείτε να κάνετε ping το `customer1.org` αν δεν υπάρχει για αυτό εγγραφή τύπου A.

Το τελευταίο πράγμα που πρέπει να κάνετε, είναι να ορίσετε στο sendmail που εκτελείται στο δικό

σας mailhost, για ποιους τομείς ή / και μηχανήματα θα δέχεται mail. Υπάρχουν μερικοί διαφορετικοί τρόποι για να γίνει αυτό. Μπορείτε να χρησιμοποιήσετε έναν από τους παρακάτω:

- Προσθέστε τα μηχανήματα στο αρχείο /etc/mail/local-host-names αν χρησιμοποιείτε τη δυνατότητα `FEATURE(use_cw_file)`. Αν χρησιμοποιείτε κάποια έκδοση του sendmail πριν την 8.10, το αρχείο είναι το /etc/sendmail.cw.
- Προσθέστε μια γραμμή `Cwyour.host.com` στο αρχείο σας /etc/sendmail.cf ή στο αρχείο /etc/mail/sendmail.cf αν χρησιμοποιείτε την έκδοση 8.10 του sendmail ή κάποια μεταγενέστερη.

53.7. SMTP με UUCP

Η προεπιλεγμένη ρύθμιση του sendmail που έρχεται με το FreeBSD, προορίζεται για δικτυακές τοποθεσίες που είναι απευθείας συνδεδεμένες στο Internet. Σε περιπτώσεις που είναι επιθυμητή η ανταλλαγή email μέσω UUCP, θα πρέπει να χρησιμοποιηθεί διαφορετικό αρχείο ρυθμίσεων για το sendmail.

Η χειροκίνητη ρύθμιση του αρχείου /etc/mail/sendmail.cf ανήκει στα προχωρημένα θέματα. Η έκδοση 8 του sendmail παράγει αρχεία ρυθμίσεων μέσω του προεπεξεργαστή m4(1), όπου οι ρυθμίσεις γίνονται σε ένα ανώτερο επίπεδο αφαίρεσης. Μπορείτε να βρείτε τα αρχεία ρύθμισης τουm4(1) στον κατάλογο /usr/shared/sendmail/cf. Διαβάστε το README στον κατάλογο cf για μια βασική εισαγωγή στις ρυθμίσεις του m4(1).

Ο καλύτερος τρόπος για την παράδοση mail μέσω του UUCP, είναι με την χρήση της δυνατότητας `mailertable`. Παράγεται με αυτό τον τρόπο μια βάση δεδομένων που μπορεί να χρησιμοποιήσει το sendmail για να πάρει αποφάσεις σχετικά με την δρομολόγηση.

Θα πρέπει αρχικά να δημιουργήσετε το αρχείο .mc. Θα βρείτε μερικά παραδείγματα στον κατάλογο /usr/shared/sendmail/cf/cf. Υποθέτοντας ότι έχετε ονομάσει το αρχείο σας foo.mc, το μόνο που χρειάζεται να κάνετε για να το μετατρέψετε σε ένα έγκυρο αρχείο sendmail.cf είναι:

```
# cd /etc/mail
# make foo.cf
# cp foo.cf /etc/mail/sendmail.cf
```

Ένα τυπικό αρχείο .mc θα δείχνει όπως το παρακάτω:

```
VERSIONID(`Your version number') OSTYPE(bsd4.4)

FEATURE(accept_unresolvable_domains)
FEATURE(nocanonify)
FEATURE(mailertable, `hash -o /etc/mail/mailertable')

define(`UUCP_RELAY', your.uucp.relay)
define(`UUCP_MAX_SIZE', 200000)
define(`confDONT_PROBE_INTERFACES')

MAILER(local)
```

```
MAILER(smtp)
MAILER(uucp)

Cw    your.alias.host.name
Cw    youruucpnodename.UUCP
```

Οι γραμμές που περιέχουν τις δυνατότητες `accept_unresolvable_domains`, `nocanonify`, and `confDONT_PROBE_INTERFACES` θα αποτρέψουν τη χρήση του DNS κατά την παράδοση του mail. Η οδηγία `UUCP_RELAY` απαιτείται για την υποστήριξη παράδοσης μέσω του UUCP. Απλώς τοποθετήστε εκεί ένα όνομα μηχανήματος στο Internet που να μπορεί να χειριστεί διευθύνσεις ψευδο-τομέων .UUCP. Το πιο πιθανό είναι να βάλετε εκεί τον αναμεταδότη (relay) για mail που παρέχει ο ISP σας.

Έχοντας κάνει το παραπάνω, θα χρειαστείτε ένα αρχείο /etc/mail/mailertable. Αν έχετε μόνο μια σύνδεση με τον έξω κόσμο που χρησιμοποιείται για όλα σας τα mail, το παρακάτω αρχείο είναι επαρκές:

```
#
# makemap hash /etc/mail/mailertable.db < /etc/mail/mailertable
.                           uucp-dom:your.uucp.relay
```

Ένα πιο πολύπλοκο παράδειγμα θα μοιάζει με το παρακάτω:

```
#
# makemap hash /etc/mail/mailertable.db < /etc/mail/mailertable
#
horus.interface-business.de   uucp-dom:horus
.interface-business.de        uucp-dom:if-bus
interface-business.de         uucp-dom:if-bus
.heep.sax.de                  smtp8:%1
horus.UUCP                    uucp-dom:horus
if-bus.UUCP                   uucp-dom:if-bus
.                             uucp-dom:
```

Οι τρεις πρώτες γραμμές χειρίζονται ειδικές περιπτώσεις, όπου το mail που απευθύνεται σε κάποιο τομέα δεν θα πρέπει να σταλθεί στην προεπιλεγμένη διαδρομή, αλλά αντίθετα σε κάποιο γειτονικό UUCP προκειμένου να "συντομευθεί" το μονοπάτι παράδοσης. Η επόμενη γραμμή χειρίζεται το mail προς τον τοπικό τομέα Ethernet, όπου είναι δυνατή η παράδοση μέσω SMTP. Τέλος, οι γειτονικοί UUCP αναφέρονται με γραφή ψευδο-τομέων UUCP ώστε να επιτρέπεται σε κάποιον `uucp-neighbor !recipient` να παρακάμψει τους προεπιλεγμένους κανόνες. Η τελευταία γραμμή είναι πάντα μια μοναδική τελεία, η οποία ταιριάζει με οτιδήποτε άλλο, με παράδοση UUCP σε ένα γειτονικό UUCP ο οποίος ενεργεί ως γενική πύλη mail προς τον υπόλοιπο κόσμο. Όλα τα ονόματα υπολογιστών που βρίσκονται μετά το `uucp-dom:` θα πρέπει να είναι έγκυροι UUCP γείτονες, όπως μπορείτε να βεβαιώσετε χρησιμοποιώντας το `uuname`.

Σας υπενθυμίζουμε ότι αυτό το αρχείο πρέπει να μετατραπεί σε μια βάση δεδομένων DBM πριν χρησιμοποιηθεί. Μπορείτε να βάλετε τη γραμμή εντολών που απαιτείται για να επιτευχθεί αυτό ως σχόλιο στην αρχή του αρχείου mailertable. Πρέπει πάντοτε να εκτελείτε αυτή την εντολή κάθε φορά

που αλλάζετε το αρχείο mailertable.

Μια τελευταία υπόδειξη: αν δεν είστε βέβαιοι για το αν θα λειτουργήσει κάποια συγκεκριμένη δρομολόγηση mail, θυμηθείτε την επιλογή `-bt` του sendmail. Αυτή ξεκινάει το sendmail σε *κατάσταση δοκιμής διευθύνσεων*. Γράψτε `3,0`, ακολουθούμενο από τη διεύθυνση που θέλετε να ελέγξετε για δρομολόγηση mail. Η τελευταία γραμμή θα σας πει τον εσωτερικό αντιπρόσωπο mail που χρησιμοποιήθηκε, τη διεύθυνση προορισμού με την οποία κλήθηκε, καθώς και την (πιθανώς μεταφρασμένη) διεύθυνση. Μπορείτε να βγείτε από αυτή την κατάσταση, πληκτρολογώντας `Ctrl` + `D`.

```
% sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 foo@example.com
canonify           input: foo @ example . com
...
parse            returns: $# uucp-dom $@ your.uucp.relay $: foo < @ example . com . >
> ^D
```

53.8. Ρύθμιση Εξυπηρετητή Μόνο για Αποστολή

Υπάρχουν πολλές περιπτώσεις, που μπορεί να θέλετε μόνο να στέλνετε mail μέσω κάποιου αναμεταδότη. Μερικά παραδείγματα:

- Ο υπολογιστής σας χρησιμοποιείται ως desktop, αλλά θέλετε να χρησιμοποιήσετε προγράμματα όπως το send-pr(1). Για να γίνει αυτό θα πρέπει να χρησιμοποιήσετε τον αναμεταδότη mail που παρέχει ο ISP σας.
- Ο υπολογιστής σας είναι ένας εξυπηρετητής που δεν χειρίζεται το mail τοπικά, αλλά χρειάζεται να το δώσει εξ' ολοκλήρου σε κάποιο αναμεταδότη για επεξεργασία.

Οποιοδήποτε σχεδόν MTA είναι ικανό να καλύψει τον παραπάνω ρόλο. Δυστυχώς, μπορεί να είναι πολύ δύσκολο να ρυθμίσετε σωστά ένα πλήρες MTA ώστε απλώς να στέλνει το mail προς αναμετάδοση. Προγράμματα όπως το sendmail και το postfix είναι υπερβολικά μεγάλα για αυτή τη δουλειά.

Επιπρόσθετα, αν χρησιμοποιείτε κάποια συνηθισμένη υπηρεσία πρόσβασης στο Internet, η συμφωνία με την εταιρία παροχής μπορεί να σας απαγορεύει να εκτελείτε το δικό σας "εξυπηρετητή mail".

Ο ευκολότερος τρόπος για να εκπληρώσετε αυτές τις ανάγκες είναι να εγκαταστήσετε το port mail/ssmtp Εκτελέστε τις ακόλουθες εντολές ως `root`:

```
# cd /usr/ports/mail/ssmtp
# make install replace clean
```

Μετά την εγκατάσταση, το mail/ssmtp μπορεί να ρυθμιστεί με ένα αρχείο τεσσάρων μόλις γραμμών, το οποίο βρίσκεται στο /usr/local/etc/ssmtp/ssmtp.conf:

```
root=yourrealemail@example.com
mailhub=mail.example.com
rewriteDomain=example.com
hostname=_HOSTNAME_
```

Βεβαιωθείτε ότι χρησιμοποιείτε την πραγματική διεύθυνση email για τον `root`. Βάλτε τον αναμεταδότη mail του ISP σας στη θέση `mail.example.com` (μερικοί ISP τον ονομάζουν "εξυπηρετητή εξερχόμενου ταχυδρομείου" ή "εξυπηρετητή SMTP").

Βεβαιωθείτε ότι έχετε απενεργοποιήσει πλήρως το sendmail, ακόμα και την υπηρεσία εξερχόμενων μηνυμάτων. Δείτε το Απενεργοποιήστε το sendmail για λεπτομέρειες.

Υπάρχουν κάποιες ακόμα διαθέσιμες επιλογές στο mail/ssmtp. Δείτε το παράδειγμα του αρχείου ρυθμίσεων στο /usr/local/etc/ssmtp ή τη σελίδα manual του ssmtp για περισσότερα παραδείγματα και πληροφορίες.

Ρυθμίζοντας το ssmtp με αυτό τον τρόπο, θα είναι δυνατή η σωστή λειτουργία οποιουδήποτε λογισμικού στον υπολογιστή σας που χρειάζεται να στείλει mail. Επίσης δεν παραβιάζεται με αυτό τον τρόπο η άδεια χρήσης του ISP σας και δεν μπορεί ο υπολογιστής σας να παραβιαστεί και να χρησιμοποιηθεί για την αποστολή ανεπιθύμητων μηνυμάτων (spam).

53.9. Χρησιμοποιώντας το Mail Μέσω Επιλογικής (Dialup) Σύνδεσης

Αν έχετε στατική διεύθυνση IP, δεν θα χρειαστεί να αλλάξετε καμιά από τις προεπιλογές. Ρυθμίστε το όνομα του υπολογιστή σας ώστε να ταιριάζει με αυτό που σας έχει οριστεί για το Internet, και το sendmail θα κάνει τα υπόλοιπα.

Αν λαμβάνετε δυναμική IP και χρησιμοποιείτε επιλογική PPP σύνδεση με το Internet, πιθανόν διαθέτετε μια θυρίδα ταχυδρομείου (mailbox) στον εξυπηρετητή mail του παροχέα σας. Ας υποθέσουμε ότι ο τομέας του ISP σας είναι `example.net`, και ότι το όνομα χρήστη σας είναι `user`, το μηχάνημα σας λέγεται `bsd.home`, και ο ISP σας, σας έχει πει ότι μπορείτε να χρησιμοποιήσετε το `relay.example.net` ως αναμεταδότη για το mail.

Για να μπορέσετε να λάβετε mail από τη θυρίδα σας, θα χρειαστείτε κάποιο αντιπρόσωπο ανάληψης (retrieval agent). Το βοηθητικό πρόγραμμα fetchmail είναι μια καλή επιλογή, καθώς υποστηρίζει πολλά διαφορετικά πρωτόκολλα. Το πρόγραμμα αυτό είναι διαθέσιμο ως πακέτο ή από την Συλλογή των Ports (mail/fetchmail). Συνήθως, ο ISP σας θα παρέχει την υπηρεσία POP. Αν χρησιμοποιείτε PPP χρήστη, μπορείτε να κατεβάσετε αυτόματα το mail σας μετά την αποκατάσταση της σύνδεσης σας, χρησιμοποιώντας την ακόλουθη καταχώριση στο /etc/ppp/ppp.linkup:

```
MYADDR:
!bg su user -c fetchmail
```

Αν χρησιμοποιείτε το sendmail (όπως φαίνεται παρακάτω) για να παραδώσετε mail σε μη-τοπικούς λογαριασμούς, πιθανόν να θέλετε το sendmail να επεξεργάζεται την ουρά του mail αμέσως μετά την

αποκατάσταση της σύνδεσης. Για να το κάνετε αυτό, βάλτε την παρακάτω εντολή αμέσως μετά την εντολή `fetchmail` στο αρχείο /etc/ppp/ppp.linkup:

```
  !bg su user -c "sendmail -q"
```

Ας υποθέσουμε ότι υπάρχει ένας λογαριασμός για τον `user` στον `bsd.home`. Στον προσωπικό κατάλογο του `user` στο `bsd.home`, δημιουργήστε ένα αρχείο .fetchmailrc:

```
poll example.net protocol pop3 fetchall pass MySecret
```

Το αρχείο αυτό δεν θα πρέπει να είναι αναγνώσιμο από κανένα, εκτός από τον `user`, καθώς περιέχει τον κωδικό `MySecret`.

Για να μπορείτε να στείλετε mail με τη σωστή επικεφαλίδα `from:`, θα πρέπει να ρυθμίσετε το sendmail να χρησιμοποιεί το user@example.net αντί για το user@bsd.home. Ίσως επίσης να θέλετε να ρυθμίσετε το sendmail να στέλνει όλο το mail μέσω του `relay.example.net`, ώστε η μετάδοση του mail να είναι ταχύτερη.

Το ακόλουθο αρχείο .mc θα πρέπει να είναι επαρκές:

```
VERSIONID(`bsd.home.mc version 1.0')
OSTYPE(bsd4.4)dnl
FEATURE(nouucp)dnl
MAILER(local)dnl
MAILER(smtp)dnl
Cwlocalhost
Cwbsd.home
MASQUERADE_AS(`example.net')dnl
FEATURE(allmasquerade)dnl
FEATURE(masquerade_envelope)dnl
FEATURE(nocanonify)dnl
FEATURE(nodns)dnl
define(`SMART_HOST', `relay.example.net')
Dmbsd.home
define(`confDOMAIN_NAME',`bsd.home')dnl
define(`confDELIVERY_MODE',`deferred')dnl
```

Διαβάστε την προηγούμενη ενότητα για λεπτομέρειες σχετικά με την μετατροπή αυτού του αρχείου .mc σε ένα αρχείο sendmail.cf. Επίσης, μη ξεχάσετε να επανεκκινήσετε το sendmail μετά την ενημέρωση του sendmail.cf.

53.10. Πιστοποίηση Αυθεντικότητας στο SMTP

Η χρήση SMTP με πιστοποίηση αυθεντικότητας στον εξυπηρετητή ταχυδρομείου σας, μπορεί να σας προσφέρει μια σειρά από οφέλη. Μπορεί να προσθέσει ένα ακόμα επίπεδο ασφάλειας στο sendmail, ενώ έχει και το πλεονέκτημα ότι δίνει τη δυνατότητα στους χρήστες φορητών υπολογιστών (που

συχνά συνδέονται μέσω διαφορετικών δικτύων) να χρησιμοποιούν τον ίδιο εξυπηρετητή ταχυδρομείου χωρίς την ανάγκη επαναρύθμισης κάθε φορά του προγράμματος αποστολής / λήψης ταχυδρομείου.

1. Εγκαταστήστε το security/cyrus-sasl2 από τη Συλλογή των Ports. Το port αυτό υποστηρίζει μια σειρά από επιλογές που μπορείτε να θέσετε κατά την μεταγλώττιση. Για να μπορέσετε να χρησιμοποιήσετε την μέθοδο αυθεντικοποίησης στο SMTP που συζητάμε εδώ, βεβαιωθείτε ότι είναι ενεργοποιημένη η επιλογή `LOGIN`.

2. Μετά την εγκατάσταση του security/cyrus-sasl2, τροποποιήστε το αρχείο /usr/local/lib/sasl2/Sendmail.conf (ή δημιουργήστε το αν δεν υπάρχει) και προσθέστε την παρακάτω γραμμή:

   ```
   pwcheck_method: saslauthd
   ```

3. Εγκαταστήστε έπειτα το security/cyrus-sasl2-saslauthd, και προσθέστε στο /etc/rc.conf την ακόλουθη γραμμή:

   ```
   saslauthd_enable="YES"
   ```

   Τέλος, ξεκινήστε το δαίμονα saslauthd:

   ```
   # /usr/local/etc/rc.d/saslauthd start
   ```

   Ο δαίμονας αυτός δρα ως ενδιάμεσος για το sendmail ώστε να γίνεται πιστοποίηση αυθεντικότητας μέσω της βάσης δεδομένων κωδικών passwd του FreeBSD συστήματος σας. Με αυτό τον τρόπο απαλλάσσεστε από την ανάγκη δημιουργίας νέου σετ από ονόματα χρηστών και κωδικούς για κάθε χρήστη που χρειάζεται να χρησιμοποιήσει πιστοποίηση στο SMTP. Χρησιμοποιείται το ίδιο όνομα και κωδικός, τόσο για είσοδο στο σύστημα, όσο και για το mail.

4. Επεξεργαστείτε τώρα το /etc/make.conf και προσθέστε τις ακόλουθες γραμμές:

   ```
   SENDMAIL_CFLAGS=-I/usr/local/include/sasl -DSASL
   SENDMAIL_LDFLAGS=-L/usr/local/lib
   SENDMAIL_LDADD=-lsasl2
   ```

   Οι γραμμές αυτές, παρέχουν στο sendmail τις κατάλληλες ρυθμίσεις ώστε να συνδεθεί σωστά με το cyrus-sasl2 κατά τη διάρκεια της μεταγλώττισης. Βεβαιωθείτε ότι είναι εγκατεστημένο το πακέτο cyrus-sasl2 πριν ξεκινήσετε την επαναμεταγλώττιση του sendmail.

5. Επαναμεταγλωττίστε το sendmail εκτελώντας τις παρακάτω εντολές:

   ```
   # cd /usr/src/lib/libsmutil
   # make cleandir && make obj && make
   # cd /usr/src/lib/libsm
   ```

```
# make cleandir && make obj && make
# cd /usr/src/usr.sbin/sendmail
# make cleandir && make obj && make && make install
```

Η μεταγλώττιση του sendmail δεν πρέπει να παρουσιάσει προβλήματα, αν το /usr/src δεν έχει αλλάξει σε μεγάλο βαθμό και εφόσον υπάρχουν οι κοινόχρηστες βιβλιοθήκες που απαιτούνται.

6. Μετά την μεταγλώττιση και επανεγκατάσταση του sendmail, επεξεργαστείτε το αρχείο /etc/mail/freebsd.mc (ή όποιο αρχείο χρησιμοποιείτε ως .mc. Πολλοί διαχειριστές επιλέγουν να χρησιμοποιήσουν την έξοδο της εντολής hostname(1) ως όνομα για το αρχείο .mc για να εξασφαλίσουν ότι είναι μοναδικό). Προσθέστε σε αυτό τις ακόλουθες γραμμές:

   ```
   dnl set SASL options
   TRUST_AUTH_MECH(`GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dnl
   define(`confAUTH_MECHANISMS', `GSSAPI DIGEST-MD5 CRAM-MD5 LOGIN')dnl
   ```

   Οι επιλογές αυτές ρυθμίζουν τις διαφορετικές μεθόδους που έχει στη διάθεση του το sendmail, προκειμένου να πιστοποιήσει τους χρήστες. Αν θέλετε να χρησιμοποιήσετε κάποια μέθοδο διαφορετική από το pwcheck, δείτε την τεκμηρίωση που περιλαμβάνεται.

7. Τέλος, εκτελέστε make(1) ενώ βρίσκεστε στον κατάλογο /etc/mail. Με τον τρόπο αυτό, θα χρησιμοποιηθεί το νέο σας .mc αρχείο και θα δημιουργηθεί ένα αρχείο .cf με όνομα freebsd.cf (ή οτιδήποτε όνομα είχατε δώσει στο αρχείο .mc). Χρησιμοποιήστε έπειτα την εντολή `make install restart`, η οποία θα αντιγράψει το αρχείο στο sendmail.cf, και θα επανεκκινήσει σωστά το sendmail. Για περισσότερες λεπτομέρειες σχετικά με αυτή τη διαδικασία, θα πρέπει να διαβάσετε το αρχείο /etc/mail/Makefile.

Αν όλα πήγαν καλά, θα πρέπει να μπορείτε να δώσετε τα στοιχεία εισόδου σας στο πρόγραμμα που χρησιμοποιείτε για αποστολή και λήψη mail, και να στείλετε ένα δοκιμαστικό μήνυμα. Για να διερευνήσετε περισσότερο τη λειτουργία, θέστε την επιλογή `LogLevel` του sendmail στο 13 και παρακολουθήστε το /var/log/maillog για τυχόν λάθη.

Για περισσότερες πληροφορίες, παρακαλούμε να δείτε τη σελίδα του sendmail που αφορά την πιστοποίηση αυθεντικότητας στο SMTP.

53.11. Προγράμματα Ταχυδρομείου για τον Χρήστη

Ένα πρόγραμμα Αντιπροσώπου Ταχυδρομείου Χρήστη (Mail User Agent, MUA), είναι μια εφαρμογή που χρησιμοποιείται για την αποστολή και λήψη email. Επιπλέον, καθώς το email "εξελίσσεται" και γίνεται πιο πολύπλοκο, τα MUA γίνονται όλο και ισχυρότερα όσο αφορά τον τρόπο που αλληλεπιδρούν με το email. Αυτό δίνει στους χρήστες περισσότερες λειτουργίες και ευελιξία. Το FreeBSD περιέχει υποστήριξη για μεγάλο αριθμό από προγράμματα ταχυδρομείου, και όλα μπορούν να εγκατασταθούν πολύ εύκολα μέσω της Συλλογής των Ports του FreeBSD. Οι χρήστες μπορούν να επιλέξουν μεταξύ γραφικών προγραμμάτων, όπως το evolution ή το balsa, και προγράμματα κονσόλας όπως τα mutt, alpine ή `mail`, ή ακόμα και τις διεπαφές web που προσφέρονται από μερικούς μεγάλους οργανισμούς.

53.11.1. mail

Το mail(1) είναι το προεπιλεγμένο πρόγραμμα ταχυδρομείου (MUA) in FreeBSD. Πρόκειται για ένα MUA κονσόλας, το οποίο προσφέρει όλες τις βασικές λειτουργίες που απαιτούνται για την αποστολή και λήψη email σε μορφή κειμένου, αν και έχει περιορισμένες δυνατότητες όσο αφορά συνημμένα αρχεία και υποστηρίζει μόνο τοπικές θυρίδες.

Αν και το `mail` δεν υποστηρίζει εγγενώς τη λήψη email μέσω διακομιστών POP ή IMAP, είναι ωστόσο δυνατόν να κατεβάσετε τα email σε μια τοπική θυρίδα (mbox) χρησιμοποιώντας κάποια εφαρμογή όπως το fetchmail, το οποίο θα συζητήσουμε αργότερα σε αυτό το κεφάλαιο (Χρησιμοποιώντας το fetchmail).

Για την αποστολή και λήψη email, εκτελέστε την εντολή `mail`:

```
% mail
```

Τα περιεχόμενα της θυρίδας του χρήστη στον κατάλογο /var/mail θα διαβαστούν αυτόματα από το πρόγραμμα `mail`. Αν η θυρίδα ταχυδρομείου είναι άδεια, το πρόγραμμα τερματίζεται με το μήνυμα ότι δεν βρέθηκε αλληλογραφία. Μετά την ανάγνωση της θυρίδας, ξεκινά η διεπαφή της εφαρμογής και εμφανίζεται μια λίστα με μηνύματα. Τα μηνύματα αριθμούνται αυτόματα, όπως φαίνεται στο παρακάτω παράδειγμα:

```
Mail version 8.1 6/6/93.  Type ? for help.
"/var/mail/marcs": 3 messages 3 new
>N  1 root@localhost        Mon Mar  8 14:05  14/510   "test"
 N  2 root@localhost        Mon Mar  8 14:05  14/509   "user account"
 N  3 root@localhost        Mon Mar  8 14:05  14/509   "sample"
```

Τα μηνύματα μπορούν πλέον να διαβαστούν με την εντολή `t` της εντολής `mail`, ακολουθούμενη με τον αριθμό του mail που θέλετε να εμφανιστεί. Στο παράδειγμα αυτό θα διαβάσουμε το πρώτο μήνυμα:

```
& t 1
Message 1:
From root@localhost  Mon Mar  8 14:05:52 2004
X-Original-To: marcs@localhost
Delivered-To: marcs@localhost
To: marcs@localhost
Subject: test
Date: Mon,  8 Mar 2004 14:05:52 +0200 (SAST)
From: root@localhost (Charlie Root)

This is a test message, please reply if you receive it.
```

Όπως φαίνεται στο παραπάνω παράδειγμα, η χρήση του πλήκτρου `t` θα προκαλέσει την εμφάνιση του μηνύματος με πλήρεις επικεφαλίδες. Για να δείτε ξανά τη λίστα με τα μηνύματα, χρησιμοποιήστε το πλήκτρο `h`.

Αν το mail απαιτεί απάντηση, μπορείτε να χρησιμοποιήσετε την εντολή `mail` χρησιμοποιώντας τις ενσωματωμένες εντολές `R` ή `r`. Το πλήκτρο `R` οδηγεί το `mail` να απαντήσει μόνο στον αποστολέα του μηνύματος, ενώ το `r` απαντάει όχι μόνο στον αποστολέα, αλλά σε όλους τους παραλήπτες του μηνύματος. Μπορείτε επίσης να προσθέσετε μετά από τις εντολές αυτές, τον αριθμό του μηνύματος στο οποίο θέλετε να απαντήσετε. Αφού το κάνετε αυτό, θα πρέπει να γράψετε την απάντηση σας και να σημειώσετε το τέλος της γράφοντας μια μόνο `.` σε μια νέα γραμμή. Μπορείτε να δείτε ένα παράδειγμα παρακάτω:

```
& R 1
To: root@localhost
Subject: Re: test

Thank you, I did get your email.
.
EOT
```

Για να στείλετε νέο mail, θα πρέπει να χρησιμοποιήσετε το πλήκτρο `m`, ακολουθούμενο από την διεύθυνση του παραλήπτη. Μπορείτε να δώσετε πολλαπλούς παραλήπτες, χωρίζοντας μεταξύ τους τις διευθύνσεις με `,`. Μπορείτε έπειτα να βάλετε το θέμα του μηνύματος και να συνεχίσετε με το περιεχόμενο. Το τέλος του μηνύματος καθορίζεται γράφοντας μια μοναδική `.` σε μια νέα γραμμή.

```
& mail root@localhost
Subject: I mastered mail

Now I can send and receive email using mail ... :)
.
EOT
```

Όσο βρίσκεστε μέσα στην εντολή `mail`, μπορείτε να χρησιμοποιήσετε το πλήκτρο `?` για την εμφάνιση βοήθειας οποιαδήποτε στιγμή. Μπορείτε επίσης να συμβουλευτείτε την σελίδα manual του mail(1) για περισσότερες πληροφορίες σχετικά με την εντολή `mail`.

Όπως αναφέραμε προηγουμένως, η εντολή mail(1) δεν σχεδιάστηκε αρχικά για να χειρίζεται συνημμένα, και για το λόγο αυτό οι δυνατότητες τις στο συγκεκριμένο θέμα είναι μικρές. Νεώτερα MUA, όπως το mutt, χειρίζονται τα συνημμένα με πολύ πιο έξυπνο τρόπο. Αλλά αν παρ' όλα αυτά επιθυμείτε να χρησιμοποιήσετε την εντολή `mail`, μάλλον θα σας φανεί χρήσιμο το port converters/mpack.

53.11.2. mutt

Το mutt είναι ένα μικρό, αλλά πολύ ισχυρό πρόγραμμα αποστολής και λήψης mail, με εξαιρετικά χαρακτηριστικά τα οποία περιλαμβάνουν:

- Την ικανότητα να δείχνει μηνύματα με την μορφή συζητήσεων
- Υποστήριξη PGP για ψηφιακή υπογραφή και κρυπτογράφηση email
- Υποστήριξη MIME

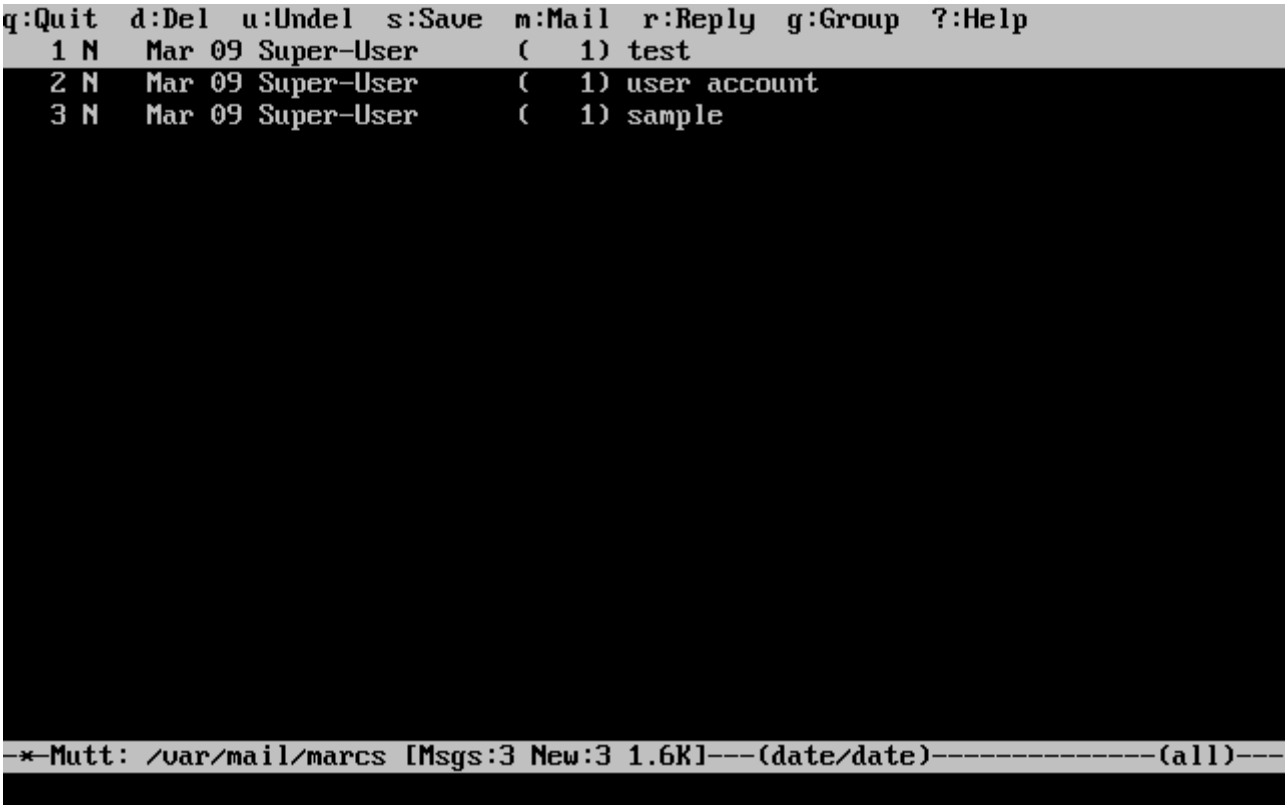
- Υποστήριξη Maildir
- Εξαιρετικές δυνατότητες παραμετροποίησης

Όλες αυτές οι δυνατότητες, κάνουν το mutt ένα από τα πιο εξελιγμένα διαθέσιμα προγράμματα ταχυδρομείου. Δείτε την τοποθεσία http://www.mutt.org για περισσότερες πληροφορίες σχετικά με το mutt.

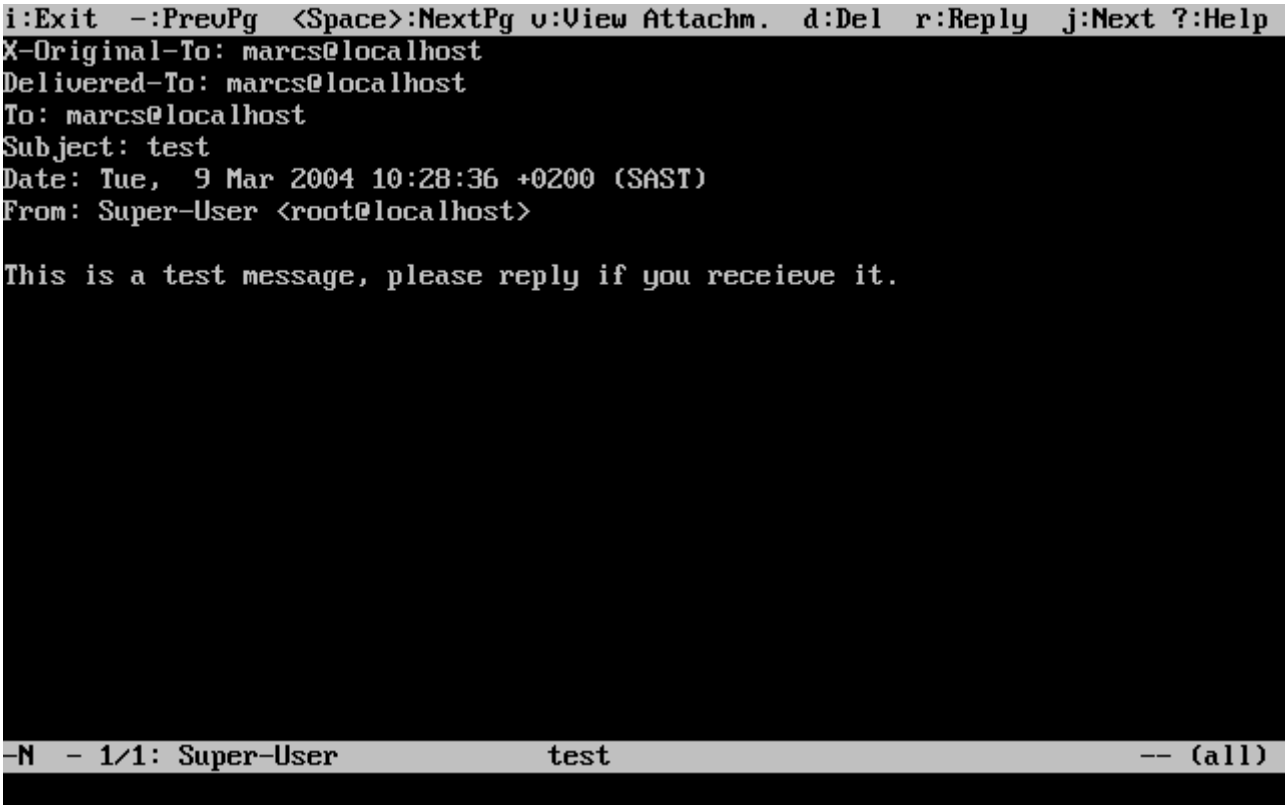
Μπορείτε να εγκαταστήσετε τη σταθερή έκδοση του mutt μέσω του port mail/mutt, ενώ και η τρέχουσα υπό εξέλιξη έκδοση είναι διαθέσιμη μέσω του port mail/mutt-devel. Μετά την εγκατάσταση του port, μπορείτε να εκτελέσετε το mutt, με την ακόλουθη εντολή:

```
% mutt
```

Το mutt θα διαβάσει αυτόματα τα περιεχόμενα της θυρίδας ταχυδρομείου χρήστη στον κατάλογο /var/mail, και θα δείξει τα περιεχόμενα του αν αυτό είναι εφικτό. Αν δεν υπάρχουν mails στη θυρίδα του χρήστη, το mutt θα εισέλθει σε κατάσταση αναμονής εντολών. Το παρακάτω παράδειγμα, δείχνει το mutt να απεικονίζει μια λίστα μηνυμάτων:



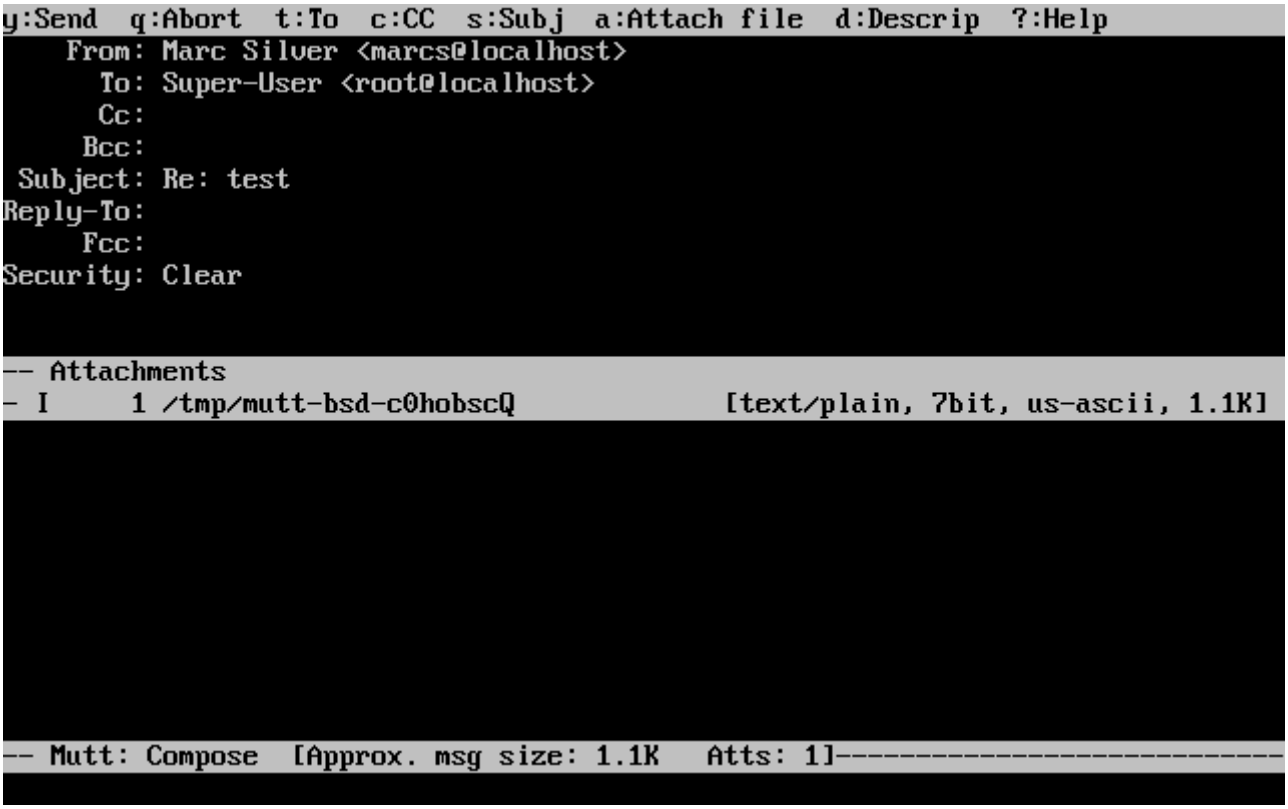
Για να διαβάσετε ένα email, επιλέξτε το χρησιμοποιώντας τα βελάκια, και πιέστε `Enter`. Μπορείτε να δείτε ένα παράδειγμα απεικόνισης mail από το mutt παρακάτω:



Όπως και το mail(1), το mutt, σας επιτρέπει να απαντήσετε τόσο στον αποστολέα του μηνύματος, όσο και σε όλους τους παραλήπτες. Για να απαντήσετε μόνο στον αποστολέα του email, χρησιμοποιήστε το πλήκτρο `r`. Για να απαντήσετε στην ομάδα χρηστών η οποία περιλαμβάνει τόσο τον αρχικό αποστολέα, όσο και τους υπόλοιπους παραλήπτες του μηνύματος, χρησιμοποιήστε το πλήκτρο `g`.

Το mutt χρησιμοποιεί το vi(1) ως συντάκτη κειμένου για δημιουργία και απάντηση σε email. Η ρύθμιση αυτή μπορεί να αλλαχθεί από το χρήστη δημιουργώντας ή τροποποιώντας το αρχείο .muttrc στον προσωπικό του κατάλογο, και θέτοντας τη μεταβλητή `editor`, ή αλλάζοντας την μεταβλητή περιβάλλοντος `EDITOR`. Δείτε την τοποθεσία http://www.mutt.org/ για περισσότερες πληροφορίες σχετικά με τη ρύθμιση του mutt.

Για να συντάξετε ένα νέο μήνυμα, πιέστε το πλήκτρο `m`. Αφού γράψετε το κατάλληλο θέμα, το mutt θα ξεκινήσει το vi(1) επιτρέποντας σας να γράψετε το mail. Μόλις ολοκληρώσετε, αποθηκεύστε και τερματίστε το `vi` και το mutt θα συνεχίσει, δείχνοντας σας μια οθόνη περίληψης του mail το οποίο πρόκειται να σταλεί. Για να στείλετε το mail, πιέστε το πλήκτρο `y`. Μπορείτε να δείτε παρακάτω ένα παράδειγμα της οθόνης περίληψης:



Το mutt περιέχει επίσης εκτεταμένη βοήθεια, στην οποία μπορείτε να έχετε πρόσβαση σχεδόν από κάθε σημείο του μενού, πιέζοντας το πλήκτρο `?`. Η γραμμή στην κορυφή της οθόνης δείχνει επίσης τις συντομεύσεις πληκτρολογίου, όπου υπάρχουν.

53.11.3. alpine

Το alpine απευθύνεται κυρίως στον αρχάριο χρήστη, αλλά περιλαμβάνει επίσης κάποια προχωρημένα χαρακτηριστικά.

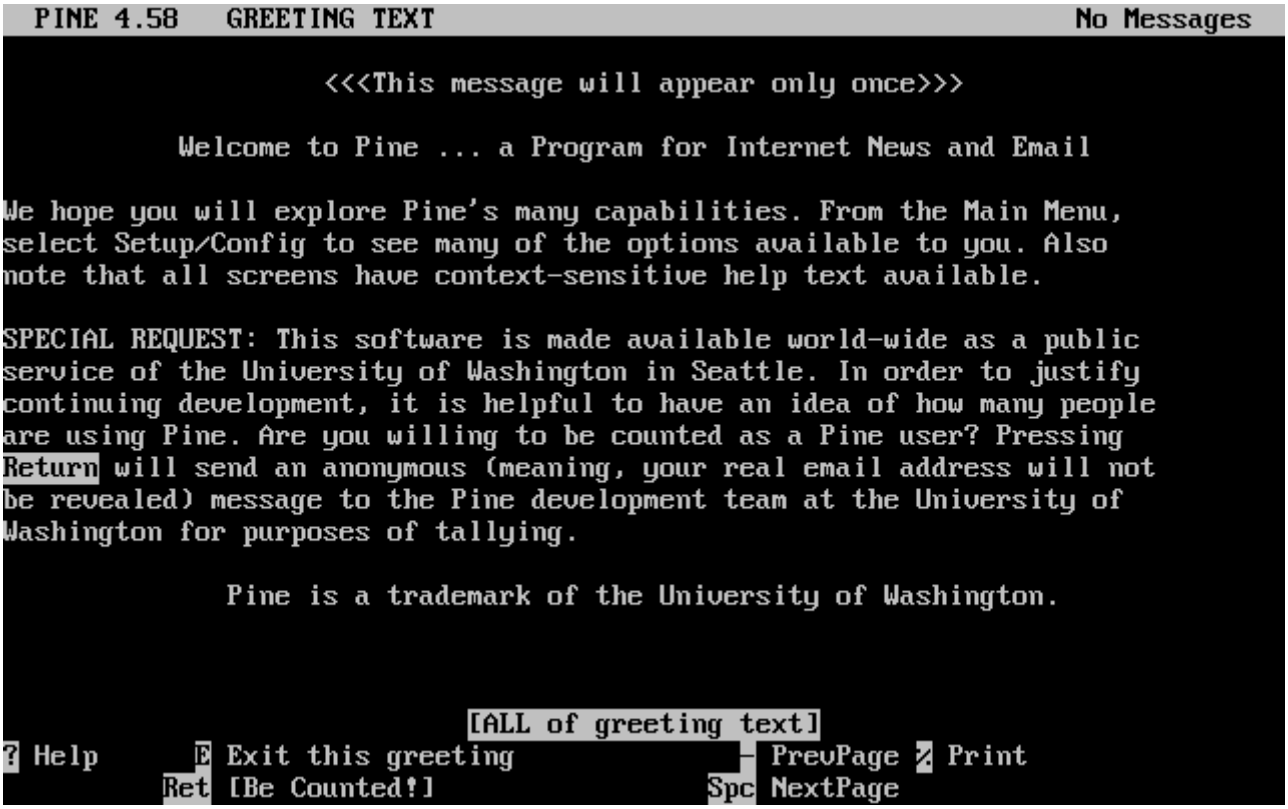
Το alpine έχει ιστορικό προβλημάτων ασφαλείας. Στο παρελθόν, ανακαλύφθηκαν προβλήματα που επέτρεπαν σε απομακρυσμένους εισβολείς να εκτελέσουν το δικό τους κώδικα στο τοπικό σύστημα, στέλνοντας απλώς ένα ειδικά διαμορφωμένο email. Όλα αυτά τα *γνωστά* προβλήματα έχουν πλέον διορθωθεί, αλλά ο κώδικας του alpine είναι γραμμένος με ιδιαίτερα ανασφαλή τρόπο, και ο Υπεύθυνος Ασφάλειας του FreeBSD, πιστεύει ότι είναι αρκετά πιθανόν να υπάρχουν και άλλα κενά ασφαλείας που δεν έχουν ανακαλυφθεί ακόμα. Εγκαταστήστε το alpine με δική σας ευθύνη.

Η τρέχουσα έκδοση του alpine μπορεί να εγκατασταθεί χρησιμοποιώντας το port mail/alpine. Μετά την εγκατάσταση του port το alpine μπορεί να ξεκινήσει χρησιμοποιώντας την παρακάτω εντολή:

```
% alpine
```

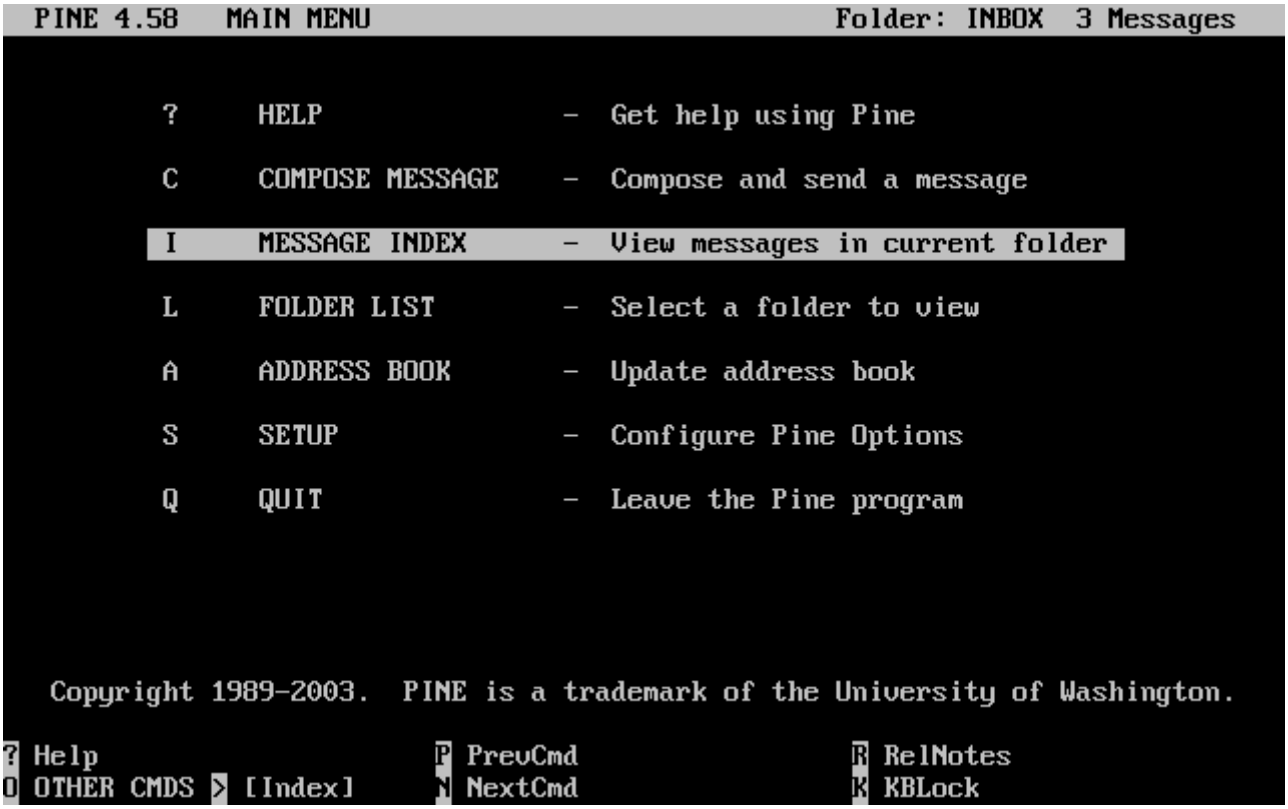
Την πρώτη φορά που θα εκτελέσετε το alpine θα σας δείξει μια αρχική σελίδα χαιρετισμού, με μια σύντομη εισαγωγή, καθώς και μια αίτηση από την ομάδα ανάπτυξης του alpine να τους στείλετε ένα ανώνυμο mail το οποίο θα τους βοηθήσει να έχουν μια ιδέα για το πόσοι χρήστες χρησιμοποιούν το λογισμικό. Για να στείλετε αυτό το ανώνυμο μήνυμα, πιέστε `Enter`, ή εναλλακτικά πιέστε `E` για να

κλείσετε την οθόνη χαιρετισμού χωρίς να στείλετε το ανώνυμο μήνυμα. Ένα παράδειγμα της σελίδας χαιρετισμού φαίνεται παρακάτω:

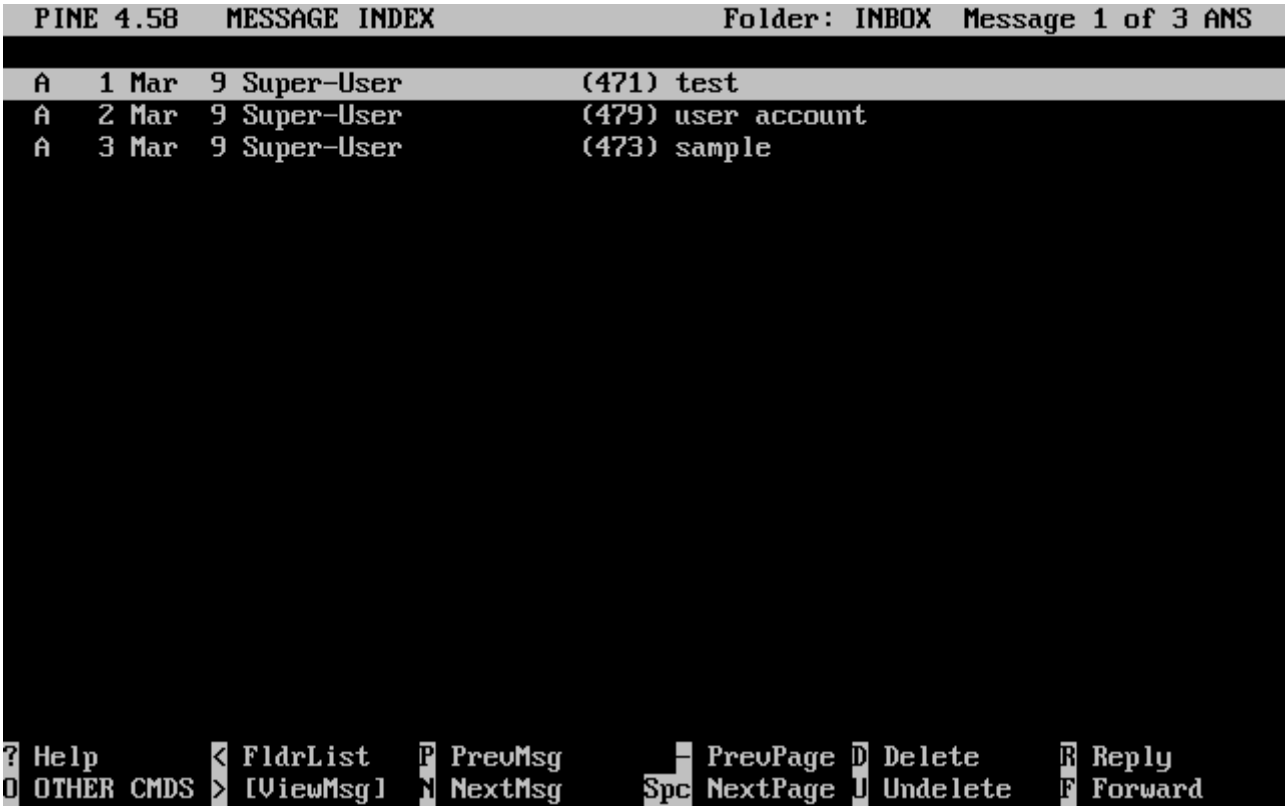


Θα εμφανιστεί κατόπιν το κύριο μενού, στο οποίο μπορείτε να μετακινηθείτε εύκολα χρησιμοποιώντας τα βελάκια. Αυτό το κύριο μενού παρέχει πλήκτρα συντόμευσης για δημιουργία νέων mail, για ανίχνευση στους καταλόγους mail, και ακόμα για διαχείριση καταχωρήσεων στο βιβλίο διευθύνσεων. Κάτω από το κύριο μενού, εμφανίζονται συντομεύσεις πληκτρολογίου σχετικές με την εργασία που γίνεται τη συγκεκριμένη στιγμή.

Ο προεπιλεγμένος κατάλογος που ανοίγει το alpine είναι το inbox. Για να δείτε το ευρετήριο των μηνυμάτων, πιέστε το `I`, ή επιλέξτε το MESSAGE INDEX όπως φαίνεται παρακάτω:

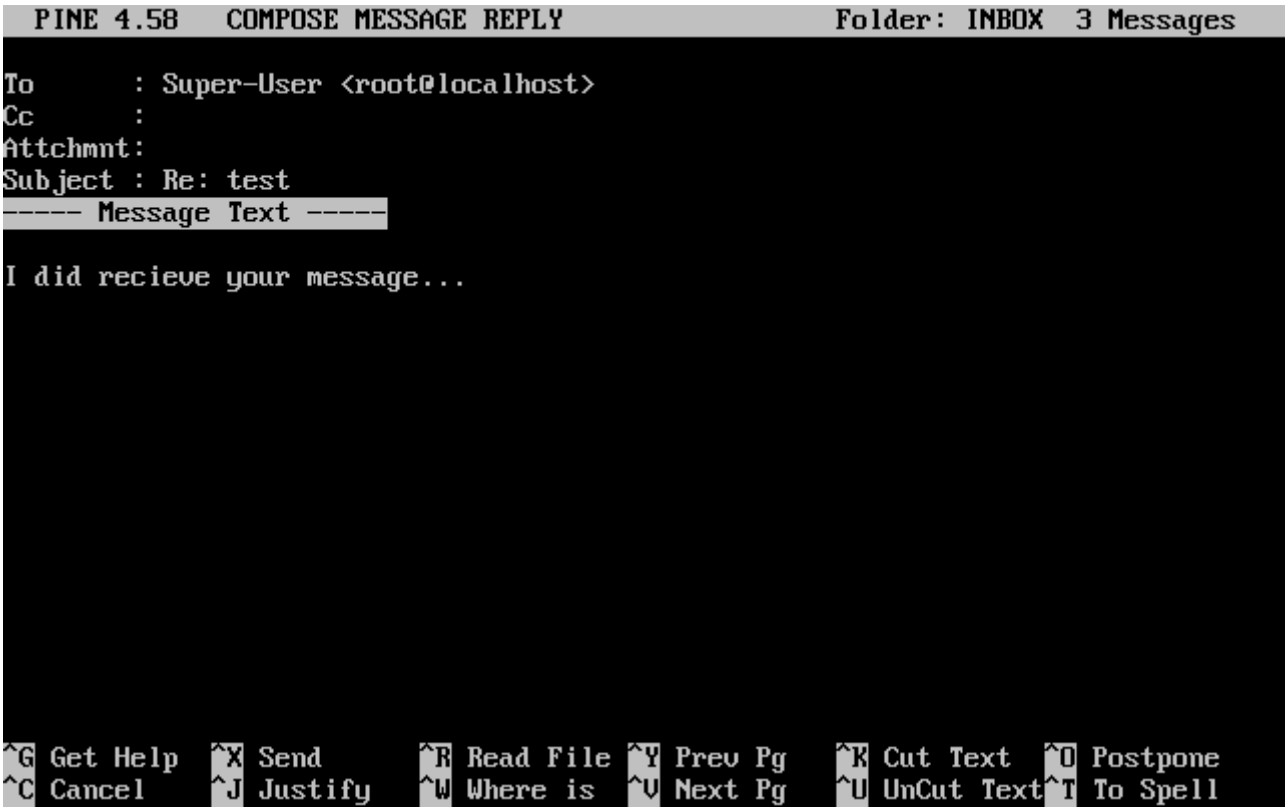


Το ευρετήριο μηνυμάτων δείχνει μηνύματα από τον τρέχοντα κατάλογο, και μπορείτε να μετακινηθείτε σε αυτό με τα βελάκια. Μπορείτε να διαβάσετε το επιλεγμένο μήνυμα, πιέζοντας το πλήκτρο `Enter`.



Στην εικόνα που φαίνεται παρακάτω, το alpine απεικονίζει ένα υπόδειγμα μηνύματος. Στο κάτω μέρος της οθόνης φαίνονται σχετικές συντομεύσεις πληκτρολογίου. Ένα παράδειγμα τέτοιας συντόμευσης, είναι το πλήκτρο `r` το οποίο λέει στο MUA να δημιουργήσει απάντηση προς το τρέχον μήνυμα που απεικονίζεται.

Η απάντηση σε ένα mail μέσω του alpine γίνεται με τη χρήση του συντάκτη κειμένου pico, ο οποίος εγκαθίσταται από προεπιλογή μαζί με το alpine. Το pico διευκολύνει τη μετακίνηση μέσα στο μήνυμα, και είναι κάπως πιο εύκολο για τους αρχάριους χρήστες σε σχέση με το vi(1) ή το mail(1). Μόλις ολοκληρώσετε την απάντηση, μπορείτε να στείλετε το μήνυμα πιέζοντας τα πλήκτρα `Ctrl` + `X`. Το alpine θα σας ζητήσει να το επιβεβαιώσετε.



Μπορείτε να προσαρμόσετε το alpine με τη χρήση της επιλογής SETUP από το κύριο μενού. Συμβουλευθείτε την τοποθεσία http://www.washington.edu/alpine/ για περισσότερες πληροφορίες.

53.12. Χρησιμοποιώντας το fetchmail

Το fetchmail είναι ένας πλήρης πελάτης για IMAP και POP, ο οποίος επιτρέπει στους χρήστες να κατεβάζουν αυτόματα mail από απομακρυσμένους εξυπηρετητές IMAP και POP και να το αποθηκεύουν σε τοπικές θυρίδες, από όπου μπορεί έπειτα να υπάρχει πιο εύκολη πρόσβαση. Το fetchmail μπορεί να εγκατασταθεί χρησιμοποιώντας το port mail/fetchmail και παρέχει διάφορα χαρακτηριστικά, μερικά από τα οποία περιλαμβάνουν:

- Υποστήριξη των πρωτοκόλλων POP3, APOP, KPOP, IMAP, ETRN και ODMR.
- Δυνατότητα προώθησης email μέσω SMTP, το οποίο επιτρέπει τη φυσιολογική λειτουργία του φιλτραρίσματος, της προώθησης, και των παρωνυμίων (aliases).
- Μπορεί να λειτουργήσει σε κατάσταση δαίμονα, ώστε να ελέγχει περιοδικά για νέα μηνύματα.
- Μπορεί να ανακτά πολλαπλές θυρίδες και να τις προωθεί, ανάλογα με τις ρυθμίσεις του, σε διαφορετικούς τοπικούς χρήστες.

Αν και είναι έξω από τους σκοπούς αυτού του κειμένου να εξηγήσει όλες τις δυνατότητες του fetchmail, θα αναφερθούμε σε κάποιες βασικές λειτουργίες. Το fetchmail χρησιμοποιεί ένα αρχείο ρυθμίσεων γνωστό ως .fetchmailrc, για να λειτουργήσει σωστά. Το αρχείο αυτό περιέχει τις πληροφορίες του εξυπηρετητή αλλά και τα στοιχεία εισόδου του χρήστη. Λόγω των ευαίσθητων πληροφοριών του αρχείου αυτού, σας συμβουλεύουμε να χρησιμοποιήσετε την παρακάτω εντολή ώστε η ανάγνωση του να επιτρέπεται μόνο από τον ιδιοκτήτη του:

```
% chmod 600 .fetchmailrc
```

Το .fetchmailrc που φαίνεται παρακάτω είναι ένα παράδειγμα με το οποίο μπορείτε να κατεβάσετε τη θυρίδα ενός χρήστη μέσω του πρωτοκόλλου POP. Κατευθύνει το fetchmail να συνδεθεί στο `example.com` χρησιμοποιώντας όνομα χρήστη `joesoap` και κωδικό `XXX`. Το παράδειγμα υποθέτει ότι ο χρήστης `joesoap` είναι επίσης και χρήστης του τοπικού συστήματος.

```
poll example.com protocol pop3 username "joesoap" password "XXX"
```

Το επόμενο παράδειγμα, δείχνει σύνδεση σε πολλαπλούς POP και IMAP εξυπηρετητές, και ανακατευθύνει σε διαφορετικούς τοπικούς χρήστες όπου είναι απαραίτητο:

```
poll example.com proto pop3:
user "joesoap", with password "XXX", is "jsoap" here;
user "andrea", with password "XXXX";
poll example2.net proto imap:
user "john", with password "XXXXX", is "myth" here;
```

Το βοηθητικό πρόγραμμα fetchmail μπορεί να λειτουργήσει σε κατάσταση δαίμονα, αν το εκτελέσετε με την επιλογή `-d`, ακολουθούμενη από ένα διάστημα (σε δευτερόλεπτα) το οποίο θα χρησιμοποιηθεί για να ερωτώνται οι εξυπηρετητές που είναι καταχωρημένοι στο αρχείο .fetchmailrc. Το παρακάτω παράδειγμα οδηγεί το fetchmail να ανιχνεύει για νέο mail κάθε 600

δευτερόλεπτα:

```
% fetchmail -d 600
```

Μπορείτε να βρείτε περισσότερες πληροφορίες για το fetchmail στην τοποθεσία http://fetchmail.berlios.de/.

53.13. Χρησιμοποιώντας το procmail

Το βοηθητικό πρόγραμμα procmail είναι μια απίστευτα ισχυρή εφαρμογή που μπορεί να χρησιμοποιηθεί για το φιλτράρισμα του εισερχόμενου mail. Επιτρέπει στους χρήστες να ορίζουν "κανόνες" οι οποίοι μπορεί να ταιριάζουν σε εισερχόμενα mail και να εκτελούν διάφορες λειτουργίες, ή να ανακατευθύνουν το mail σε εναλλακτικές θυρίδες ή / και διευθύνσεις ταχυδρομείου. Το procmail μπορεί να εγκατασταθεί χρησιμοποιώντας το port mail/procmail. Μετά την εγκατάσταση του, μπορεί να ενσωματωθεί σχεδόν σε οποιοδήποτε MTA. Συμβουλευθείτε την τεκμηρίωση του MTA που χρησιμοποιείτε για περισσότερες πληροφορίες. Εναλλακτικά, μπορείτε να ενσωματώσετε το procmail προσθέτοντας την ακόλουθη γραμμή σε ένα αρχείο .forward στον κατάλογο του χρήστη, χρησιμοποιώντας τις δυνατότητες του procmail:

```
"|exec /usr/local/bin/procmail || exit 75"
```

Στην παρακάτω ενότητα, θα δείξουμε μερικούς από τους βασικούς κανόνες του procmail, καθώς και σύντομες περιγραφές της λειτουργίας τους. Πρέπει να τοποθετήσετε αυτούς (και άλλους) κανόνες σε ένα αρχείο .procmailrc, το οποίο θα πρέπει να βρίσκεται μέσα στον κατάλογο του χρήστη:

Μπορείτε να βρείτε τους περισσότερους από αυτούς τους κανόνες, στη σελίδα manual του procmailex(5).

Προώθηση όλου του email της διεύθυνσης user@example.com προς την εξωτερική διεύθυνση goodmail@example2.com:

```
:0
* ^From.*user@example.com
! goodmail@example2.com
```

Προώθηση όλων των email που είναι μικρότερα από 1000 bytes προς μια εξωτερική διεύθυνση email goodmail@example2.com:

```
:0
* < 1000
! goodmail@example2.com
```

Αποστολή όλου του mail που στάλθηκε προς το alternate@example.com σε μια θυρίδα που καλείται alternate:

```
:0
* ^TOalternate@example.com
alternate
```

Αποστολή όλου του mail με θέμα "Spam" προς το /dev/null:

```
:0
^Subject:.*Spam
/dev/null
```

Μια χρήσιμη λύση που ξεχωρίζει τα email από τις λίστες ταχυδρομείου `FreeBSD.org` και τοποθετεί το κάθε μήνυμα σε διαφορετική θυρίδα:

```
:0
* ^Sender:.owner-freebsd-\/[^@]+@FreeBSD.ORG
{
    LISTNAME=${MATCH}
    :0
    * LISTNAME??^\/[^@]+
    FreeBSD-${MATCH}
}
```

Chapter 54. Εξυπηρετητές Δικτύου

54.1. Σύνοψη

Το κεφάλαιο αυτό καλύπτει ορισμένες από τις πιο συχνά χρησιμοποιούμενες δικτυακές υπηρεσίες των συστημάτων UNIX®. Θα παρουσιάσουμε την εγκατάσταση, ρύθμιση, έλεγχο και συντήρηση πολλών διαφορετικών τύπων δικτυακών υπηρεσιών. Σε όλο το κεφάλαιο, για τη δική σας διευκόλυνση, υπάρχουν παραδείγματα διαφόρων αρχείων ρυθμίσεων.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να διαχειρίζεστε την υπηρεσία inetd.
- Πως να ρυθμίσετε ένα δικτυακό σύστημα αρχείων.
- Πως να ρυθμίσετε ένα εξυπηρετητή δικτυακών πληροφοριών για το διαμοιρασμό λογαριασμών χρηστών.
- Πως να χρησιμοποιήσετε το DHCP για την αυτόματη ρύθμιση των παραμέτρων του δικτύου.
- Πως να ρυθμίσετε ένα εξυπηρετητή ονομασίας περιοχών (DNS).
- Πως να ρυθμίσετε τον εξυπηρετητή ιστοσελίδων Apache.
- Πως να ρυθμίσετε ένα εξυπηρετητή μεταφοράς αρχείων (FTP).
- Πως να ρυθμίσετε ένα εξυπηρετητή αρχείων και εκτυπωτών για πελάτες Windows® με χρήση της εφαρμογής Samba.
- Πως να συγχρονίσετε την ημερομηνία και την ώρα, και να ρυθμίσετε ένα εξυπηρετητή ώρας με τη βοήθεια του NTP πρωτοκόλλου.

Πριν διαβάσετε αυτό κεφάλαιο, θα πρέπει:

- Να κατανοείτε τις βασικές έννοιες των αρχείων script /etc/rc.
- Να είστε εξοικειωμένοι με τη βασική ορολογία των δικτύων.
- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

54.2. The inetd"Super-Server"

54.2.1. Overview

inetd(8) is sometimes referred to as the "Internet Super-Server" because it manages connections for several services. When a connection is received by inetd, it determines which program the connection is destined for, spawns the particular process and delegates the socket to it (the program is invoked with the service socket as its standard input, output and error descriptors). Running inetd for servers that are not heavily used can reduce the overall system load, when compared to running each daemon individually in stand-alone mode.

Primarily, inetd is used to spawn other daemons, but several trivial protocols are handled directly,

such as chargen, auth, and daytime.

This section will cover the basics in configuring inetd through its command-line options and its configuration file, /etc/inetd.conf.

54.2.2. Settings

inetd is initialized through the rc(8) system. The `inetd_enable` option is set to `NO` by default, but may be turned on by sysinstall during installation, depending on the configuration chosen by the user. Placing:

```
inetd_enable="YES"
```

or

```
inetd_enable="NO"
```

into /etc/rc.conf will enable or disable inetd starting at boot time. The command:

```
/etc/rc.d/inetd rcvar
```

can be run to display the current effective setting.

Additionally, different command-line options can be passed to inetd via the `inetd_flags` option.

54.2.3. Command-Line Options

Like most server daemons, inetd has a number of options that it can be passed in order to modify its behaviour. The full list of options reads:

```
inetd [-d] [-l] [-w] [-W] [-c maximum] [-C rate] [-a address | hostname] [-p filename] [-R rate] [-s maximum] [configuration file]
```

Options can be passed to inetd using the `inetd_flags` option in /etc/rc.conf. By default, `inetd_flags` is set to `-wW -C 60`, which turns on TCP wrapping for inetd's services, and prevents any single IP address from requesting any service more than 60 times in any given minute.

Novice users may be pleased to note that these parameters usually do not need to be modified, although we mention the rate-limiting options below as they be useful should you find that you are receiving an excessive amount of connections. A full list of options can be found in the inetd(8) manual.

-c maximum

Specify the default maximum number of simultaneous invocations of each service; the default is unlimited. May be overridden on a per-service basis with the `max-child` parameter.

-C rate

Specify the default maximum number of times a service can be invoked from a single IP address in one minute; the default is unlimited. May be overridden on a per-service basis with the `max-connections-per-ip-per-minute` parameter.

-R rate

Specify the maximum number of times a service can be invoked in one minute; the default is 256. A rate of 0 allows an unlimited number of invocations.

-s maximum

Specify the maximum number of times a service can be invoked from a single IP address at any one time; the default is unlimited. May be overridden on a per-service basis with the `max-child-per-ip` parameter.

54.2.4. inetd.conf

Configuration of inetd is done via the file /etc/inetd.conf.

When a modification is made to /etc/inetd.conf, inetd can be forced to re-read its configuration file by running the command:

Παράδειγμα 24. Reloading the inetd configuration file

```
# /etc/rc.d/inetd reload
```

Each line of the configuration file specifies an individual daemon. Comments in the file are preceded by a "#". The format of each entry in /etc/inetd.conf is as follows:

```
service-name
socket-type
protocol
{wait|nowait}[/max-child[/max-connections-per-ip-per-minute[/max-child-per-ip]]]
user[:group][/login-class]
server-program
server-program-arguments
```

An example entry for the ftpd(8) daemon using IPv4 might read:

```
ftp     stream  tcp     nowait  root    /usr/libexec/ftpd       ftpd -l
```

service-name

This is the service name of the particular daemon. It must correspond to a service listed in /etc/services. This determines which port inetd must listen to. If a new service is being created, it must be placed in /etc/services first.

socket-type

Either `stream`, `dgram`, `raw`, or `seqpacket`. `stream` must be used for connection-based, TCP daemons, while `dgram` is used for daemons utilizing the UDP transport protocol.

protocol

One of the following:

Protocol	Explanation
tcp, tcp4	TCP IPv4
udp, udp4	UDP IPv4
tcp6	TCP IPv6
udp6	UDP IPv6
tcp46	Both TCP IPv4 and v6
udp46	Both UDP IPv4 and v6

{wait|nowait}[/max-child[/max-connections-per-ip-per-minute[/max-child-per-ip]]]

`wait|nowait` indicates whether the daemon invoked from inetd is able to handle its own socket or not. `dgram` socket types must use the `wait` option, while stream socket daemons, which are usually multi-threaded, should use `nowait`. `wait` usually hands off multiple sockets to a single daemon, while `nowait` spawns a child daemon for each new socket.

The maximum number of child daemons inetd may spawn can be set using the `max-child` option. If a limit of ten instances of a particular daemon is needed, a `/10` would be placed after `nowait`. Specifying `/0` allows an unlimited number of children

In addition to `max-child`, two other options which limit the maximum connections from a single place to a particular daemon can be enabled. `max-connections-per-ip-per-minute` limits the number of connections from any particular IP address per minutes, e.g. a value of ten would limit any particular IP address connecting to a particular service to ten attempts per minute. `max-child-per-ip` limits the number of children that can be started on behalf on any single IP address at any moment. These options are useful to prevent intentional or unintentional excessive resource consumption and Denial of Service (DoS) attacks to a machine.

In this field, either of `wait` or `nowait` is mandatory. `max-child`, `max-connections-per-ip-per-minute` and `max-child-per-ip` are optional.

A stream-type multi-threaded daemon without any `max-child`, `max-connections-per-ip-per-minute` or `max-child-per-ip` limits would simply be: `nowait`.

The same daemon with a maximum limit of ten daemons would read: `nowait/10`.

The same setup with a limit of twenty connections per IP address per minute and a maximum total limit of ten child daemons would read: `nowait/10/20`.

These options are utilized by the default settings of the fingerd(8) daemon, as seen here:

```
finger stream  tcp     nowait/3/10 nobody /usr/libexec/fingerd fingerd -s
```

Finally, an example of this field with a maximum of 100 children in total, with a maximum of 5 for any one IP address would read: `nowait/100/0/5`.

user

This is the username that the particular daemon should run as. Most commonly, daemons run as the `root` user. For security purposes, it is common to find some servers running as the `daemon` user, or the least privileged `nobody` user.

server-program

The full path of the daemon to be executed when a connection is received. If the daemon is a service provided by inetd internally, then `internal` should be used.

server-program-arguments

This works in conjunction with `server-program` by specifying the arguments, starting with `argv[0]`, passed to the daemon on invocation. If `mydaemon -d` is the command line, `mydaemon -d` would be the value of `server-program-arguments`. Again, if the daemon is an internal service, use `internal` here.

54.2.5. Security

Depending on the choices made at install time, many of inetd's services may be enabled by default. If there is no apparent need for a particular daemon, consider disabling it. Place a "#" in front of the daemon in question in /etc/inetd.conf, and then reload the inetd configuration. Some daemons, such as fingerd, may not be desired at all because they provide information that may be useful to an attacker.

Some daemons are not security-conscious and have long, or non-existent, timeouts for connection attempts. This allows an attacker to slowly send connections to a particular daemon, thus saturating available resources. It may be a good idea to place `max-connections-per-ip-per-minute`, `max-child` or `max-child-per-ip` limitations on certain daemons if you find that you have too many connections.

By default, TCP wrapping is turned on. Consult the hosts_access(5) manual page for more information on placing TCP restrictions on various inetd invoked daemons.

54.2.6. Miscellaneous

daytime, time, echo, discard, chargen, and auth are all internally provided services of inetd.

The auth service provides identity network services, and is configurable to a certain degree, whilst the others are simply on or off.

Consult the inetd(8) manual page for more in-depth information.

54.3. Network File System (NFS)

Among the many different file systems that FreeBSD supports is the Network File System, also known as NFS. NFS allows a system to share directories and files with others over a network. By using NFS, users and programs can access files on remote systems almost as if they were local files.

Some of the most notable benefits that NFS can provide are:

- Local workstations use less disk space because commonly used data can be stored on a single machine and still remain accessible to others over the network.
- There is no need for users to have separate home directories on every network machine. Home directories could be set up on the NFS server and made available throughout the network.
- Storage devices such as floppy disks, CDROM drives, and Zip® drives can be used by other machines on the network. This may reduce the number of removable media drives throughout the network.

54.3.1. How NFS Works

NFS consists of at least two main parts: a server and one or more clients. The client remotely accesses the data that is stored on the server machine. In order for this to function properly a few processes have to be configured and running.

The server has to be running the following daemons:

Daemon	Description
nfsd	The NFS daemon which services requests from the NFS clients.
mountd	The NFS mount daemon which carries out the requests that nfsd(8) passes on to it.
rpcbind	This daemon allows NFS clients to discover which port the NFS server is using.

The client can also run a daemon, known as nfsiod. The nfsiod daemon services the requests from the NFS server. This is optional, and improves performance, but is not required for normal and correct operation. See the nfsiod(8) manual page for more information.

54.3.2. Configuring NFS

NFS configuration is a relatively straightforward process. The processes that need to be running can all start at boot time with a few modifications to your /etc/rc.conf file.

On the NFS server, make sure that the following options are configured in the /etc/rc.conf file:

```
rpcbind_enable="YES"
nfs_server_enable="YES"
mountd_flags="-r"
```

mountd runs automatically whenever the NFS server is enabled.

On the client, make sure this option is present in /etc/rc.conf:

```
nfs_client_enable="YES"
```

The /etc/exports file specifies which file systems NFS should export (sometimes referred to as "share"). Each line in /etc/exports specifies a file system to be exported and which machines have access to that file system. Along with what machines have access to that file system, access options may also be specified. There are many such options that can be used in this file but only a few will be mentioned here. You can easily discover other options by reading over the exports(5) manual page.

Here are a few example /etc/exports entries:

The following examples give an idea of how to export file systems, although the settings may be different depending on your environment and network configuration. For instance, to export the /cdrom directory to three example machines that have the same domain name as the server (hence the lack of a domain name for each) or have entries in your /etc/hosts file. The `-ro` flag makes the exported file system read-only. With this flag, the remote system will not be able to write any changes to the exported file system.

```
/cdrom -ro host1 host2 host3
```

The following line exports /home to three hosts by IP address. This is a useful setup if you have a private network without a DNS server configured. Optionally the /etc/hosts file could be configured for internal hostnames; please review hosts(5) for more information. The `-alldirs` flag allows the subdirectories to be mount points. In other words, it will not mount the subdirectories but permit the client to mount only the directories that are required or needed.

```
/home  -alldirs  10.0.0.2 10.0.0.3 10.0.0.4
```

The following line exports /a so that two clients from different domains may access the file system. The `-maproot=root` flag allows the `root` user on the remote system to write data on the exported file system as `root`. If the `-maproot=root` flag is not specified, then even if a user has `root` access on the remote system, he will not be able to modify files on the exported file system.

```
/a  -maproot=root  host.example.com box.example.org
```

In order for a client to access an exported file system, the client must have permission to do so. Make sure the client is listed in your /etc/exports file.

In /etc/exports, each line represents the export information for one file system to one host. A remote host can only be specified once per file system, and may only have one default entry. For example, assume that /usr is a single file system. The following /etc/exports would be invalid:

```
# Invalid when /usr is one file system
/usr/src   client
/usr/ports client
```

One file system, /usr, has two lines specifying exports to the same host, `client`. The correct format for this situation is:

```
/usr/src /usr/ports  client
```

The properties of one file system exported to a given host must all occur on one line. Lines without a client specified are treated as a single host. This limits how you can export file systems, but for most people this is not an issue.

The following is an example of a valid export list, where /usr and /exports are local file systems:

```
# Export src and ports to client01 and client02, but only
# client01 has root privileges on it
/usr/src /usr/ports -maproot=root    client01
/usr/src /usr/ports               client02
# The client machines have root and can mount anywhere
# on /exports. Anyone in the world can mount /exports/obj read-only
/exports -alldirs -maproot=root      client01 client02
/exports/obj -ro
```

The mountd daemon must be forced to recheck the /etc/exports file whenever it has been modified, so the changes can take effect. This can be accomplished either by sending a HUP signal to the running daemon:

```
# kill -HUP `cat /var/run/mountd.pid`
```

or by invoking the `mountd` rc(8) script with the appropriate parameter:

```
# /etc/rc.d/mountd onereload
```

Please refer to Χρησιμοποιώντας Το Σύστημα rc Στο FreeBSD for more information about using rc scripts.

Alternatively, a reboot will make FreeBSD set everything up properly. A reboot is not necessary though. Executing the following commands as `root` should start everything up.

On the NFS server:

```
# rpcbind
# nfsd -u -t -n 4
```

```
# mountd -r
```

On the NFS client:

```
# nfsiod -n 4
```

Now everything should be ready to actually mount a remote file system. In these examples the server's name will be `server` and the client's name will be `client`. If you only want to temporarily mount a remote file system or would rather test the configuration, just execute a command like this as `root` on the client:

```
# mount server:/home /mnt
```

This will mount the /home directory on the server at /mnt on the client. If everything is set up correctly you should be able to enter /mnt on the client and see all the files that are on the server.

If you want to automatically mount a remote file system each time the computer boots, add the file system to the /etc/fstab file. Here is an example:

```
server:/home    /mnt    nfs rw  0   0
```

The fstab(5) manual page lists all the available options.

54.3.3. Locking

Some applications (e.g. mutt) require file locking to operate correctly. In the case of NFS, rpc.lockd can be used for file locking. To enable it, add the following to the /etc/rc.conf file on both client and server (it is assumed that the NFS client and server are configured already):

```
rpc_lockd_enable="YES"
rpc_statd_enable="YES"
```

Start the application by using:

```
# /etc/rc.d/nfslocking start
```

If real locking between the NFS clients and NFS server is not required, it is possible to let the NFS client do locking locally by passing `-L` to mount_nfs(8). Refer to the mount_nfs(8) manual page for further details.

54.3.4. Practical Uses

NFS has many practical uses. Some of the more common ones are listed below:

- Set several machines to share a CDROM or other media among them. This is cheaper and often a more convenient method to install software on multiple machines.
- On large networks, it might be more convenient to configure a central NFS server in which to store all the user home directories. These home directories can then be exported to the network so that users would always have the same home directory, regardless of which workstation they log in to.
- Several machines could have a common /usr/ports/distfiles directory. That way, when you need to install a port on several machines, you can quickly access the source without downloading it on each machine.

54.3.5. Automatic Mounts with amd

amd(8) (the automatic mounter daemon) automatically mounts a remote file system whenever a file or directory within that file system is accessed. Filesystems that are inactive for a period of time will also be automatically unmounted by amd. Using amd provides a simple alternative to permanent mounts, as permanent mounts are usually listed in /etc/fstab.

amd operates by attaching itself as an NFS server to the /host and /net directories. When a file is accessed within one of these directories, amd looks up the corresponding remote mount and automatically mounts it. /net is used to mount an exported file system from an IP address, while /host is used to mount an export from a remote hostname.

An access to a file within /host/foobar/usr would tell amd to attempt to mount the /usr export on the host `foobar`.

Παράδειγμα 25. Mounting an Export with amd

You can view the available mounts of a remote host with the `showmount` command. For example, to view the mounts of a host named `foobar`, you can use:

```
% showmount -e foobar
Exports list on foobar:
/usr                               10.10.10.0
/a                                 10.10.10.0
% cd /host/foobar/usr
```

As seen in the example, the `showmount` shows /usr as an export. When changing directories to /host/foobar/usr, amd attempts to resolve the hostname `foobar` and automatically mount the desired export.

amd can be started by the startup scripts by placing the following lines in /etc/rc.conf:

```
amd_enable="YES"
```

Additionally, custom flags can be passed to amd from the `amd_flags` option. By default, `amd_flags` is set to:

```
amd_flags="-a /.amd_mnt -l syslog /host /etc/amd.map /net /etc/amd.map"
```

The /etc/amd.map file defines the default options that exports are mounted with. The /etc/amd.conf file defines some of the more advanced features of amd.

Consult the amd(8) and amd.conf(8) manual pages for more information.

54.3.6. Problems Integrating with Other Systems

Certain Ethernet adapters for ISA PC systems have limitations which can lead to serious network problems, particularly with NFS. This difficulty is not specific to FreeBSD, but FreeBSD systems are affected by it.

The problem nearly always occurs when (FreeBSD) PC systems are networked with high-performance workstations, such as those made by Silicon Graphics, Inc., and Sun Microsystems, Inc. The NFS mount will work fine, and some operations may succeed, but suddenly the server will seem to become unresponsive to the client, even though requests to and from other systems continue to be processed. This happens to the client system, whether the client is the FreeBSD system or the workstation. On many systems, there is no way to shut down the client gracefully once this problem has manifested itself. The only solution is often to reset the client, because the NFS situation cannot be resolved.

Though the "correct" solution is to get a higher performance and capacity Ethernet adapter for the FreeBSD system, there is a simple workaround that will allow satisfactory operation. If the FreeBSD system is the *server*, include the option `-w=1024` on the mount from the client. If the FreeBSD system is the *client*, then mount the NFS file system with the option `-r=1024`. These options may be specified using the fourth field of the fstab entry on the client for automatic mounts, or by using the `-o` parameter of the mount(8) command for manual mounts.

It should be noted that there is a different problem, sometimes mistaken for this one, when the NFS servers and clients are on different networks. If that is the case, make *certain* that your routers are routing the necessary UDP information, or you will not get anywhere, no matter what else you are doing.

In the following examples, `fastws` is the host (interface) name of a high-performance workstation, and `freebox` is the host (interface) name of a FreeBSD system with a lower-performance Ethernet adapter. Also, /sharedfs will be the exported NFS file system (see exports(5)), and /project will be the mount point on the client for the exported file system. In all cases, note that additional options, such as `hard` or `soft` and `bg` may be desirable in your application.

Examples for the FreeBSD system (`freebox`) as the client in /etc/fstab on `freebox`:

```
fastws:/sharedfs /project nfs rw,-r=1024 0 0
```

As a manual mount command on `freebox`:

```
# mount -t nfs -o -r=1024 fastws:/sharedfs /project
```

Examples for the FreeBSD system as the server in /etc/fstab on `fastws`:

```
freebox:/sharedfs /project nfs rw,-w=1024 0 0
```

As a manual mount command on `fastws`:

```
# mount -t nfs -o -w=1024 freebox:/sharedfs /project
```

Nearly any 16-bit Ethernet adapter will allow operation without the above restrictions on the read or write size.

For anyone who cares, here is what happens when the failure occurs, which also explains why it is unrecoverable. NFS typically works with a "block" size of 8 K (though it may do fragments of smaller sizes). Since the maximum Ethernet packet is around 1500 bytes, the NFS "block" gets split into multiple Ethernet packets, even though it is still a single unit to the upper-level code, and must be received, assembled, and *acknowledged* as a unit. The high-performance workstations can pump out the packets which comprise the NFS unit one right after the other, just as close together as the standard allows. On the smaller, lower capacity cards, the later packets overrun the earlier packets of the same unit before they can be transferred to the host and the unit as a whole cannot be reconstructed or acknowledged. As a result, the workstation will time out and try again, but it will try again with the entire 8 K unit, and the process will be repeated, ad infinitum.

By keeping the unit size below the Ethernet packet size limitation, we ensure that any complete Ethernet packet received can be acknowledged individually, avoiding the deadlock situation.

Overruns may still occur when a high-performance workstations is slamming data out to a PC system, but with the better cards, such overruns are not guaranteed on NFS "units". When an overrun occurs, the units affected will be retransmitted, and there will be a fair chance that they will be received, assembled, and acknowledged.

54.4. Network Information System (NIS/YP)

54.4.1. What Is It?

NIS, which stands for Network Information Services, was developed by Sun Microsystems to centralize administration of UNIX® (originally SunOS™) systems. It has now essentially become an industry standard; all major UNIX® like systems (Solaris™, HP-UX, AIX®, Linux, NetBSD, OpenBSD, FreeBSD, etc) support NIS.

NIS was formerly known as Yellow Pages, but because of trademark issues, Sun changed the name. The old term (and yp) is still often seen and used.

It is a RPC-based client/server system that allows a group of machines within an NIS domain to share a common set of configuration files. This permits a system administrator to set up NIS client

systems with only minimal configuration data and add, remove or modify configuration data from a single location.

It is similar to the Windows NT® domain system; although the internal implementation of the two are not at all similar, the basic functionality can be compared.

54.4.2. Terms/Processes You Should Know

There are several terms and several important user processes that you will come across when attempting to implement NIS on FreeBSD, whether you are trying to create an NIS server or act as an NIS client:

Term	Description
NIS domainname	An NIS master server and all of its clients (including its slave servers) have a NIS domainname. Similar to an Windows NT® domain name, the NIS domainname does not have anything to do with DNS.
rpcbind	Must be running in order to enable RPC (Remote Procedure Call, a network protocol used by NIS). If rpcbind is not running, it will be impossible to run an NIS server, or to act as an NIS client.
ypbind	"Binds" an NIS client to its NIS server. It will take the NIS domainname from the system, and using RPC, connect to the server. ypbind is the core of client-server communication in an NIS environment; if ypbind dies on a client machine, it will not be able to access the NIS server.
ypserv	Should only be running on NIS servers; this is the NIS server process itself. If ypserv(8) dies, then the server will no longer be able to respond to NIS requests (hopefully, there is a slave server to take over for it). There are some implementations of NIS (but not the FreeBSD one), that do not try to reconnect to another server if the server it used before dies. Often, the only thing that helps in this case is to restart the server process (or even the whole server) or the ypbind process on the client.
rpc.yppasswdd	Another process that should only be running on NIS master servers; this is a daemon that will allow NIS clients to change their NIS passwords. If this daemon is not running, users will have to login to the NIS master server and change their passwords there.

54.4.3. How Does It Work?

There are three types of hosts in an NIS environment: master servers, slave servers, and clients. Servers act as a central repository for host configuration information. Master servers hold the authoritative copy of this information, while slave servers mirror this information for redundancy. Clients rely on the servers to provide this information to them.

Information in many files can be shared in this manner. The master.passwd, group, and hosts files are commonly shared via NIS. Whenever a process on a client needs information that would normally be found in these files locally, it makes a query to the NIS server that it is bound to instead.

54.4.3.1. Machine Types

- A *NIS master server*. This server, analogous to a Windows NT® primary domain controller, maintains the files used by all of the NIS clients. The passwd, group, and other various files used by the NIS clients live on the master server.

It is possible for one machine to be an NIS master server for more than one NIS domain. However, this will not be covered in this introduction, which assumes a relatively small-scale NIS environment.

- *NIS slave servers*. Similar to the Windows NT® backup domain controllers, NIS slave servers maintain copies of the NIS master's data files. NIS slave servers provide the redundancy, which is needed in important environments. They also help to balance the load of the master server: NIS Clients always attach to the NIS server whose response they get first, and this includes slave-server-replies.
- *NIS clients*. NIS clients, like most Windows NT® workstations, authenticate against the NIS server (or the Windows NT® domain controller in the Windows NT® workstations case) to log on.

54.4.4. Using NIS/YP

This section will deal with setting up a sample NIS environment.

54.4.4.1. Planning

Let us assume that you are the administrator of a small university lab. This lab, which consists of 15 FreeBSD machines, currently has no centralized point of administration; each machine has its own /etc/passwd and /etc/master.passwd. These files are kept in sync with each other only through manual intervention; currently, when you add a user to the lab, you must run `adduser` on all 15 machines. Clearly, this has to change, so you have decided to convert the lab to use NIS, using two of the machines as servers.

Therefore, the configuration of the lab now looks something like:

Machine name	IP address	Machine role
`ellington`	`10.0.0.2`	NIS master

Machine name	IP address	Machine role
coltrane	10.0.0.3	NIS slave
basie	10.0.0.4	Faculty workstation
bird	10.0.0.5	Client machine
cli[1-11]	10.0.0.[6-17]	Other client machines

If you are setting up a NIS scheme for the first time, it is a good idea to think through how you want to go about it. No matter what the size of your network, there are a few decisions that need to be made.

54.4.4.1.1. Choosing a NIS Domain Name

This might not be the "domainname" that you are used to. It is more accurately called the "NIS domainname". When a client broadcasts its requests for info, it includes the name of the NIS domain that it is part of. This is how multiple servers on one network can tell which server should answer which request. Think of the NIS domainname as the name for a group of hosts that are related in some way.

Some organizations choose to use their Internet domainname for their NIS domainname. This is not recommended as it can cause confusion when trying to debug network problems. The NIS domainname should be unique within your network and it is helpful if it describes the group of machines it represents. For example, the Art department at Acme Inc. might be in the "acme-art" NIS domain. For this example, assume you have chosen the name `test-domain`.

However, some operating systems (notably SunOS™) use their NIS domain name as their Internet domain name. If one or more machines on your network have this restriction, you *must* use the Internet domain name as your NIS domain name.

54.4.4.1.2. Physical Server Requirements

There are several things to keep in mind when choosing a machine to use as a NIS server. One of the unfortunate things about NIS is the level of dependency the clients have on the server. If a client cannot contact the server for its NIS domain, very often the machine becomes unusable. The lack of user and group information causes most systems to temporarily freeze up. With this in mind you should make sure to choose a machine that will not be prone to being rebooted regularly, or one that might be used for development. The NIS server should ideally be a stand alone machine whose sole purpose in life is to be an NIS server. If you have a network that is not very heavily used, it is acceptable to put the NIS server on a machine running other services, just keep in mind that if the NIS server becomes unavailable, it will affect *all* of your NIS clients adversely.

54.4.4.2. NIS Servers

The canonical copies of all NIS information are stored on a single machine called the NIS master server. The databases used to store the information are called NIS maps. In FreeBSD, these maps are stored in /var/yp/[domainname] where [domainname] is the name of the NIS domain being served. A single NIS server can support several domains at once, therefore it is possible to have several such directories, one for each supported domain. Each domain will have its own independent set of maps.

NIS master and slave servers handle all NIS requests with the `ypserv` daemon. `ypserv` is responsible for receiving incoming requests from NIS clients, translating the requested domain and map name to a path to the corresponding database file and transmitting data from the database back to the client.

54.4.4.2.1. Setting Up a NIS Master Server

Setting up a master NIS server can be relatively straight forward, depending on your needs. FreeBSD comes with support for NIS out-of-the-box. All you need is to add the following lines to /etc/rc.conf, and FreeBSD will do the rest for you.

```
nisdomainname="test-domain"
```

This line will set the NIS domainname to `test-domain` upon network setup (e.g. after reboot).

```
nis_server_enable="YES"
```

This will tell FreeBSD to start up the NIS server processes when the networking is next brought up.

```
nis_yppasswdd_enable="YES"
```

This will enable the `rpc.yppasswdd` daemon which, as mentioned above, will allow users to change their NIS password from a client machine.

Depending on your NIS setup, you may need to add further entries. See the section about NIS servers that are also NIS clients, below, for details.

Now, all you have to do is to run the command `/etc/netstart` as superuser. It will set up everything for you, using the values you defined in /etc/rc.conf.

54.4.4.2.2. Initializing the NIS Maps

The *NIS maps* are database files, that are kept in the /var/yp directory. They are generated from configuration files in the /etc directory of the NIS master, with one exception: the /etc/master.passwd file. This is for a good reason, you do not want to propagate passwords to your `root` and other administrative accounts to all the servers in the NIS domain. Therefore, before we initialize the NIS maps, you should:

```
# cp /etc/master.passwd /var/yp/master.passwd
# cd /var/yp
# vi master.passwd
```

You should remove all entries regarding system accounts (`bin`, `tty`, `kmem`, `games`, etc), as well as any

accounts that you do not want to be propagated to the NIS clients (for example `root` and any other UID 0 (superuser) accounts).

Make sure the /var/yp/master.passwd is neither group nor world readable (mode 600)! Use the `chmod` command, if appropriate.

When you have finished, it is time to initialize the NIS maps! FreeBSD includes a script named `ypinit` to do this for you (see its manual page for more information). Note that this script is available on most UNIX® Operating Systems, but not on all. On Digital UNIX/Compaq Tru64 UNIX it is called `ypsetup`. Because we are generating maps for an NIS master, we are going to pass the `-m` option to `ypinit`. To generate the NIS maps, assuming you already performed the steps above, run:

```
ellington# ypinit -m test-domain
Server Type: MASTER Domain: test-domain
Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.
Do you want this procedure to quit on non-fatal errors? [y/n: n] n
Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
At this point, we have to construct a list of this domains YP servers.
rod.darktech.org is already known as master server.
Please continue to add any slave servers, one per line. When you are
done with the list, type a <control D>.
master server   :  ellington
next host to add:  coltrane
next host to add:  ^D
The current list of NIS servers looks like this:
ellington
coltrane
Is this correct?  [y/n: y] y

[..output from map generation..]

NIS Map update completed.
ellington has been setup as an YP master server without any errors.
```

`ypinit` should have created /var/yp/Makefile from /var/yp/Makefile.dist. When created, this file assumes that you are operating in a single server NIS environment with only FreeBSD machines. Since `test-domain` has a slave server as well, you must edit /var/yp/Makefile:

```
ellington# vi /var/yp/Makefile
```

You should comment out the line that says

```
NOPUSH = "True"
```

(if it is not commented out already).

54.4.4.2.3. Setting up a NIS Slave Server

Setting up an NIS slave server is even more simple than setting up the master. Log on to the slave server and edit the file /etc/rc.conf as you did before. The only difference is that we now must use the `-s` option when running `ypinit`. The `-s` option requires the name of the NIS master be passed to it as well, so our command line looks like:

```
coltrane# ypinit -s ellington test-domain

Server Type: SLAVE Domain: test-domain Master: ellington

Creating an YP server will require that you answer a few questions.
Questions will all be asked at the beginning of the procedure.

Do you want this procedure to quit on non-fatal errors? [y/n: n]  n

Ok, please remember to go back and redo manually whatever fails.
If you don't, something might not work.
There will be no further questions. The remainder of the procedure
should take a few minutes, to copy the databases from ellington.
Transferring netgroup...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byuser...
ypxfr: Exiting: Map successfully transferred
Transferring netgroup.byhost...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byuid...
ypxfr: Exiting: Map successfully transferred
Transferring passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring group.bygid...
ypxfr: Exiting: Map successfully transferred
Transferring group.byname...
ypxfr: Exiting: Map successfully transferred
Transferring services.byname...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring rpc.byname...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.byname...
ypxfr: Exiting: Map successfully transferred
Transferring master.passwd.byname...
ypxfr: Exiting: Map successfully transferred
Transferring networks.byname...
ypxfr: Exiting: Map successfully transferred
```

```
Transferring networks.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring netid.byname...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byaddr...
ypxfr: Exiting: Map successfully transferred
Transferring protocols.bynumber...
ypxfr: Exiting: Map successfully transferred
Transferring ypservers...
ypxfr: Exiting: Map successfully transferred
Transferring hosts.byname...
ypxfr: Exiting: Map successfully transferred

coltrane has been setup as an YP slave server without any errors.
Don't forget to update map ypservers on ellington.
```

You should now have a directory called /var/yp/test-domain. Copies of the NIS master server's maps should be in this directory. You will need to make sure that these stay updated. The following /etc/crontab entries on your slave servers should do the job:

```
20      *       *       *       *       root    /usr/libexec/ypxfr passwd.byname
21      *       *       *       *       root    /usr/libexec/ypxfr passwd.byuid
```

These two lines force the slave to sync its maps with the maps on the master server. Although these entries are not mandatory, since the master server attempts to ensure any changes to its NIS maps are communicated to its slaves and because password information is vital to systems depending on the server, it is a good idea to force the updates. This is more important on busy networks where map updates might not always complete.

Now, run the command `/etc/netstart` on the slave server as well, which again starts the NIS server.

54.4.4.3. NIS Clients

An NIS client establishes what is called a binding to a particular NIS server using the `ypbind` daemon. `ypbind` checks the system's default domain (as set by the `domainname` command), and begins broadcasting RPC requests on the local network. These requests specify the name of the domain for which `ypbind` is attempting to establish a binding. If a server that has been configured to serve the requested domain receives one of the broadcasts, it will respond to `ypbind`, which will record the server's address. If there are several servers available (a master and several slaves, for example), `ypbind` will use the address of the first one to respond. From that point on, the client system will direct all of its NIS requests to that server. `ypbind` will occasionally "ping" the server to make sure it is still up and running. If it fails to receive a reply to one of its pings within a reasonable amount of time, `ypbind` will mark the domain as unbound and begin broadcasting again in the hopes of locating another server.

54.4.4.3.1. Setting Up a NIS Client

Setting up a FreeBSD machine to be a NIS client is fairly straightforward.

1. Edit the file /etc/rc.conf and add the following lines in order to set the NIS domainname and start `ypbind` upon network startup:

```
nisdomainname="test-domain"
nis_client_enable="YES"
```

2. To import all possible password entries from the NIS server, remove all user accounts from your /etc/master.passwd file and use `vipw` to add the following line to the end of the file:

```
+:::::::::
```

This line will afford anyone with a valid account in the NIS server's password maps an account. There are many ways to configure your NIS client by changing this line. See the netgroups section below for more information. For more detailed reading see O'Reilly's book on `Managing NFS and NIS`.

You should keep at least one local account (i.e. not imported via NIS) in your /etc/master.passwd and this account should also be a member of the group `wheel`. If there is something wrong with NIS, this account can be used to log in remotely, become `root`, and fix things.

3. To import all possible group entries from the NIS server, add this line to your /etc/group file:

```
+:*::
```

After completing these steps, you should be able to run `ypcat passwd` and see the NIS server's passwd map.

54.4.5. NIS Security

In general, any remote user can issue an RPC to ypserv(8) and retrieve the contents of your NIS maps, provided the remote user knows your domainname. To prevent such unauthorized transactions, ypserv(8) supports a feature called "securenets" which can be used to restrict access to a given set of hosts. At startup, ypserv(8) will attempt to load the securenets information from a file called /var/yp/securenets.

This path varies depending on the path specified with the `-p` option. This file contains entries that consist of a network specification and a network mask separated by white space. Lines starting with "#" are considered to be comments. A sample securenets file might look like this:

```
# allow connections from local host -- mandatory
127.0.0.1     255.255.255.255
# allow connections from any host
# on the 192.168.128.0 network
192.168.128.0 255.255.255.0
# allow connections from any host
# between 10.0.0.0 to 10.0.15.255
# this includes the machines in the testlab
10.0.0.0      255.255.240.0
```

If ypserv(8) receives a request from an address that matches one of these rules, it will process the request normally. If the address fails to match a rule, the request will be ignored and a warning message will be logged. If the /var/yp/securenets file does not exist, `ypserv` will allow connections from any host.

The `ypserv` program also has support for Wietse Venema's TCP Wrapper package. This allows the administrator to use the TCP Wrapper configuration files for access control instead of /var/yp/securenets.

While both of these access control mechanisms provide some security, they, like the privileged port test, are vulnerable to "IP spoofing" attacks. All NIS-related traffic should be blocked at your firewall.

Servers using /var/yp/securenets may fail to serve legitimate NIS clients with archaic TCP/IP implementations. Some of these implementations set all host bits to zero when doing broadcasts and/or fail to observe the subnet mask when calculating the broadcast address. While some of these problems can be fixed by changing the client configuration, other problems may force the retirement of the client systems in question or the abandonment of /var/yp/securenets.

Using /var/yp/securenets on a server with such an archaic implementation of TCP/IP is a really bad idea and will lead to loss of NIS functionality for large parts of your network.

The use of the TCP Wrapper package increases the latency of your NIS server. The additional delay may be long enough to cause timeouts in client programs, especially in busy networks or with slow NIS servers. If one or more of your client systems suffers from these symptoms, you should convert the client systems in question into NIS slave servers and force them to bind to themselves.

54.4.6. Barring Some Users from Logging On

In our lab, there is a machine `basie` that is supposed to be a faculty only workstation. We do not want to take this machine out of the NIS domain, yet the passwd file on the master NIS server contains accounts for both faculty and students. What can we do?

There is a way to bar specific users from logging on to a machine, even if they are present in the NIS database. To do this, all you must do is add `-username` to the end of the /etc/master.passwd file

on the client machine, where *username* is the username of the user you wish to bar from logging in. This should preferably be done using `vipw`, since `vipw` will sanity check your changes to /etc/master.passwd, as well as automatically rebuild the password database when you finish editing. For example, if we wanted to bar user `bill` from logging on to `basie` we would:

```
basie# vipw
[add -bill to the end, exit]
vipw: rebuilding the database...
vipw: done

basie# cat /etc/master.passwd

root:[password]:0:0::0:0:The super-user:/root:/bin/csh
toor:[password]:0:0::0:0:The other super-user:/root:/bin/sh
daemon:*:1:1::0:0:Owner of many system processes:/root:/sbin/nologin
operator:*:2:5::0:0:System &:/:/sbin/nologin
bin:*:3:7::0:0:Binaries Commands and Source,,,:/:/sbin/nologin
tty:*:4:65533::0:0:Tty Sandbox:/:/sbin/nologin
kmem:*:5:65533::0:0:KMem Sandbox:/:/sbin/nologin
games:*:7:13::0:0:Games pseudo-user:/usr/games:/sbin/nologin
news:*:8:8::0:0:News Subsystem:/:/sbin/nologin
man:*:9:9::0:0:Mister Man Pages:/usr/shared/man:/sbin/nologin
bind:*:53:53::0:0:Bind Sandbox:/:/sbin/nologin
uucp:*:66:66::0:0:UUCP pseudo-user:/var/spool/uucppublic:/usr/libexec/uucp/uucico
xten:*:67:67::0:0:X-10 daemon:/usr/local/xten:/sbin/nologin
pop:*:68:6::0:0:Post Office Owner:/nonexistent:/sbin/nologin
nobody:*:65534:65534::0:0:Unprivileged user:/nonexistent:/sbin/nologin
+:::::::::
-bill

basie#
```

54.4.7. Using Netgroups

The method shown in the previous section works reasonably well if you need special rules for a very small number of users and/or machines. On larger networks, you *will* forget to bar some users from logging onto sensitive machines, or you may even have to modify each machine separately, thus losing the main benefit of NIS: *centralized* administration.

The NIS developers' solution for this problem is called *netgroups*. Their purpose and semantics can be compared to the normal groups used by UNIX® file systems. The main differences are the lack of a numeric ID and the ability to define a netgroup by including both user accounts and other netgroups.

Netgroups were developed to handle large, complex networks with hundreds of users and machines. On one hand, this is a Good Thing if you are forced to deal with such a situation. On the other hand, this complexity makes it almost impossible to explain netgroups with really simple examples. The example used in the remainder of this section demonstrates this problem.

Let us assume that your successful introduction of NIS in your laboratory caught your superiors' interest. Your next job is to extend your NIS domain to cover some of the other machines on campus. The two tables contain the names of the new users and new machines as well as brief descriptions of them.

User Name(s)	Description
`alpha`, `beta`	Normal employees of the IT department
`charlie`, `delta`	The new apprentices of the IT department
`echo`, `foxtrott`, `golf`, ...	Ordinary employees
`able`, `baker`, ...	The current interns

Machine Name(s)	Description
`war`, `death`, `famine`, `pollution`	Your most important servers. Only the IT employees are allowed to log onto these machines.
`pride`, `greed`, `envy`, `wrath`, `lust`, `sloth`	Less important servers. All members of the IT department are allowed to login onto these machines.
`one`, `two`, `three`, `four`, ...	Ordinary workstations. Only the *real* employees are allowed to use these machines.
`trashcan`	A very old machine without any critical data. Even the intern is allowed to use this box.

If you tried to implement these restrictions by separately blocking each user, you would have to add one `-user` line to each system's passwd for each user who is not allowed to login onto that system. If you forget just one entry, you could be in trouble. It may be feasible to do this correctly during the initial setup, however you *will* eventually forget to add the lines for new users during day-to-day operations. After all, Murphy was an optimist.

Handling this situation with netgroups offers several advantages. Each user need not be handled separately; you assign a user to one or more netgroups and allow or forbid logins for all members of the netgroup. If you add a new machine, you will only have to define login restrictions for netgroups. If a new user is added, you will only have to add the user to one or more netgroups. Those changes are independent of each other: no more "for each combination of user and machine do..." If your NIS setup is planned carefully, you will only have to modify exactly one central configuration file to grant or deny access to machines.

The first step is the initialization of the NIS map netgroup. FreeBSD's ypinit(8) does not create this map by default, but its NIS implementation will support it once it has been created. To create an empty map, simply type

```
ellington# vi /var/yp/netgroup
```

and start adding content. For our example, we need at least four netgroups: IT employees, IT

apprentices, normal employees and interns.

```
IT_EMP  (,alpha,test-domain)    (,beta,test-domain)
IT_APP  (,charlie,test-domain)  (,delta,test-domain)
USERS   (,echo,test-domain)     (,foxtrott,test-domain) \
        (,golf,test-domain)
INTERNS (,able,test-domain)     (,baker,test-domain)
```

IT_EMP, IT_APP etc. are the names of the netgroups. Each bracketed group adds one or more user accounts to it. The three fields inside a group are:

1. The name of the host(s) where the following items are valid. If you do not specify a hostname, the entry is valid on all hosts. If you do specify a hostname, you will enter a realm of darkness, horror and utter confusion.
2. The name of the account that belongs to this netgroup.
3. The NIS domain for the account. You can import accounts from other NIS domains into your netgroup if you are one of the unlucky fellows with more than one NIS domain.

Each of these fields can contain wildcards. See netgroup(5) for details.

Netgroup names longer than 8 characters should not be used, especially if you have machines running other operating systems within your NIS domain. The names are case sensitive; using capital letters for your netgroup names is an easy way to distinguish between user, machine and netgroup names.

Some NIS clients (other than FreeBSD) cannot handle netgroups with a large number of entries. For example, some older versions of SunOS™ start to cause trouble if a netgroup contains more than 15 *entries*. You can circumvent this limit by creating several sub-netgroups with 15 users or less and a real netgroup that consists of the sub-netgroups:

```
BIGGRP1  (,joe1,domain)  (,joe2,domain)  (,joe3,domain) [...]
BIGGRP2  (,joe16,domain)  (,joe17,domain) [...]
BIGGRP3  (,joe31,domain)  (,joe32,domain)
BIGGROUP  BIGGRP1 BIGGRP2 BIGGRP3
```

You can repeat this process if you need more than 225 users within a single netgroup.

Activating and distributing your new NIS map is easy:

```
ellington# cd /var/yp
ellington# make
```

This will generate the three NIS maps netgroup, netgroup.byhost and netgroup.byuser. Use ypcat(1)

to check if your new NIS maps are available:

```
ellington% ypcat -k netgroup
ellington% ypcat -k netgroup.byhost
ellington% ypcat -k netgroup.byuser
```

The output of the first command should resemble the contents of /var/yp/netgroup. The second command will not produce output if you have not specified host-specific netgroups. The third command can be used to get the list of netgroups for a user.

The client setup is quite simple. To configure the server `war`, you only have to start vipw(8) and replace the line

```
+:::::::::
```

with

```
+@IT_EMP:::::::::
```

Now, only the data for the users defined in the netgroup `IT_EMP` is imported into `war`'s password database and only these users are allowed to login.

Unfortunately, this limitation also applies to the `~` function of the shell and all routines converting between user names and numerical user IDs. In other words, `cd ~user` will not work, `ls -l` will show the numerical ID instead of the username and `find . -user joe -print` will fail with `No such user`. To fix this, you will have to import all user entries *without allowing them to login onto your servers*.

This can be achieved by adding another line to /etc/master.passwd. This line should contain:

`+:::::::::/sbin/nologin`, meaning "Import all entries but replace the shell with /sbin/nologin in the imported entries". You can replace any field in the `passwd` entry by placing a default value in your /etc/master.passwd.

Make sure that the line `:::::::::/sbin/nologin` is placed after `@IT_EMP:::::::::`. Otherwise, all user accounts imported from NIS will have /sbin/nologin as their login shell.

After this change, you will only have to change one NIS map if a new employee joins the IT department. You could use a similar approach for the less important servers by replacing the old `+:::::::::` in their local version of /etc/master.passwd with something like this:

```
+@IT_EMP:::::::::
+@IT_APP:::::::::
+:::::::::/sbin/nologin
```

The corresponding lines for the normal workstations could be:

```
+@IT_EMP:::::::::
+@USERS:::::::::
+::::::::::/sbin/nologin
```

And everything would be fine until there is a policy change a few weeks later: The IT department starts hiring interns. The IT interns are allowed to use the normal workstations and the less important servers; and the IT apprentices are allowed to login onto the main servers. You add a new netgroup `IT_INTERN`, add the new IT interns to this netgroup and start to change the configuration on each and every machine... As the old saying goes: "Errors in centralized planning lead to global mess".

NIS' ability to create netgroups from other netgroups can be used to prevent situations like these. One possibility is the creation of role-based netgroups. For example, you could create a netgroup called `BIGSRV` to define the login restrictions for the important servers, another netgroup called `SMALLSRV` for the less important servers and a third netgroup called `USERBOX` for the normal workstations. Each of these netgroups contains the netgroups that are allowed to login onto these machines. The new entries for your NIS map netgroup should look like this:

```
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP  ITINTERN
USERBOX   IT_EMP  ITINTERN USERS
```

This method of defining login restrictions works reasonably well if you can define groups of machines with identical restrictions. Unfortunately, this is the exception and not the rule. Most of the time, you will need the ability to define login restrictions on a per-machine basis.

Machine-specific netgroup definitions are the other possibility to deal with the policy change outlined above. In this scenario, the /etc/master.passwd of each box contains two lines starting with "+". The first of them adds a netgroup with the accounts allowed to login onto this machine, the second one adds all other accounts with /sbin/nologin as shell. It is a good idea to use the "ALL-CAPS" version of the machine name as the name of the netgroup. In other words, the lines should look like this:

```
+@BOXNAME:::::::::
+::::::::::/sbin/nologin
```

Once you have completed this task for all your machines, you will not have to modify the local versions of /etc/master.passwd ever again. All further changes can be handled by modifying the NIS map. Here is an example of a possible netgroup map for this scenario with some additional goodies:

```
# Define groups of users first
IT_EMP    (,alpha,test-domain)    (,beta,test-domain)
IT_APP    (,charlie,test-domain)  (,delta,test-domain)
DEPT1     (,echo,test-domain)     (,foxtrott,test-domain)
```

```
DEPT2     (,golf,test-domain)     (,hotel,test-domain)
DEPT3     (,india,test-domain)    (,juliet,test-domain)
ITINTERN  (,kilo,test-domain)     (,lima,test-domain)
D_INTERNS (,able,test-domain)     (,baker,test-domain)
#
# Now, define some groups based on roles
USERS     DEPT1   DEPT2     DEPT3
BIGSRV    IT_EMP  IT_APP
SMALLSRV  IT_EMP  IT_APP    ITINTERN
USERBOX   IT_EMP  ITINTERN  USERS
#
# And a groups for a special tasks
# Allow echo and golf to access our anti-virus-machine
SECURITY  IT_EMP  (,echo,test-domain)  (,golf,test-domain)
#
# machine-based netgroups
# Our main servers
WAR       BIGSRV
FAMINE    BIGSRV
# User india needs access to this server
POLLUTION  BIGSRV  (,india,test-domain)
#
# This one is really important and needs more access restrictions
DEATH     IT_EMP
#
# The anti-virus-machine mentioned above
ONE       SECURITY
#
# Restrict a machine to a single user
TWO       (,hotel,test-domain)
# [...more groups to follow]
```

If you are using some kind of database to manage your user accounts, you should be able to create the first part of the map with your database's report tools. This way, new users will automatically have access to the boxes.

One last word of caution: It may not always be advisable to use machine-based netgroups. If you are deploying a couple of dozen or even hundreds of identical machines for student labs, you should use role-based netgroups instead of machine-based netgroups to keep the size of the NIS map within reasonable limits.

54.4.8. Important Things to Remember

There are still a couple of things that you will need to do differently now that you are in an NIS environment.

- Every time you wish to add a user to the lab, you must add it to the master NIS server *only*, and *you must remember to rebuild the NIS maps*. If you forget to do this, the new user will not be able to login anywhere except on the NIS master. For example, if we needed to add a new user `jsmith` to the lab, we would:

```
# pw useradd jsmith
# cd /var/yp
# make test-domain
```

You could also run `adduser jsmith` instead of `pw useradd jsmith`.

- *Keep the administration accounts out of the NIS maps*. You do not want to be propagating administrative accounts and passwords to machines that will have users that should not have access to those accounts.
- *Keep the NIS master and slave secure, and minimize their downtime*. If somebody either hacks or simply turns off these machines, they have effectively rendered many people without the ability to login to the lab.

  This is the chief weakness of any centralized administration system. If you do not protect your NIS servers, you will have a lot of angry users!

54.4.9. NIS v1 Compatibility

FreeBSD's ypserv has some support for serving NIS v1 clients. FreeBSD's NIS implementation only uses the NIS v2 protocol, however other implementations include support for the v1 protocol for backwards compatibility with older systems. The ypbind daemons supplied with these systems will try to establish a binding to an NIS v1 server even though they may never actually need it (and they may persist in broadcasting in search of one even after they receive a response from a v2 server). Note that while support for normal client calls is provided, this version of ypserv does not handle v1 map transfer requests; consequently, it cannot be used as a master or slave in conjunction with older NIS servers that only support the v1 protocol. Fortunately, there probably are not any such servers still in use today.

54.4.10. NIS Servers That Are Also NIS Clients

Care must be taken when running ypserv in a multi-server domain where the server machines are also NIS clients. It is generally a good idea to force the servers to bind to themselves rather than allowing them to broadcast bind requests and possibly become bound to each other. Strange failure modes can result if one server goes down and others are dependent upon it. Eventually all the clients will time out and attempt to bind to other servers, but the delay involved can be considerable and the failure mode is still present since the servers might bind to each other all over again.

You can force a host to bind to a particular server by running `ypbind` with the `-S` flag. If you do not want to do this manually each time you reboot your NIS server, you can add the following lines to your /etc/rc.conf:

```
nis_client_enable="YES" # run client stuff as well
nis_client_flags="-S NIS domain,server"
```

See ypbind(8) for further information.

54.4.11. Password Formats

One of the most common issues that people run into when trying to implement NIS is password format compatibility. If your NIS server is using DES encrypted passwords, it will only support clients that are also using DES. For example, if you have Solaris™ NIS clients in your network, then you will almost certainly need to use DES encrypted passwords.

To check which format your servers and clients are using, look at /etc/login.conf. If the host is configured to use DES encrypted passwords, then the `default` class will contain an entry like this:

```
default:\
    :passwd_format=des:\
    [Further entries elided]
```

Other possible values for the `passwd_format` capability include `blf` and `md5` (for Blowfish and MD5 encrypted passwords, respectively).

If you have made changes to /etc/login.conf, you will also need to rebuild the login capability database, which is achieved by running the following command as `root`:

```
# cap_mkdb /etc/login.conf
```

The format of passwords already in /etc/master.passwd will not be updated until a user changes his password for the first time *after* the login capability database is rebuilt.

Next, in order to ensure that passwords are encrypted with the format that you have chosen, you should also check that the `crypt_default` in /etc/auth.conf gives precedence to your chosen password format. To do this, place the format that you have chosen first in the list. For example, when using DES encrypted passwords, the entry would be:

```
crypt_default   =   des blf md5
```

Having followed the above steps on each of the FreeBSD based NIS servers and clients, you can be sure that they all agree on which password format is used within your network. If you have trouble authenticating on an NIS client, this is a pretty good place to start looking for possible problems. Remember: if you want to deploy an NIS server for a heterogenous network, you will probably have to use DES on all systems because it is the lowest common standard.

54.5. Automatic Network Configuration (DHCP)

54.5.1. What Is DHCP?

DHCP, the Dynamic Host Configuration Protocol, describes the means by which a system can connect to a network and obtain the necessary information for communication upon that network.

FreeBSD versions prior to 6.0 use the ISC (Internet Software Consortium) DHCP client (dhclient(8)) implementation. Later versions use the OpenBSD `dhclient` taken from OpenBSD 3.7. All information here regarding `dhclient` is for use with either of the ISC or OpenBSD DHCP clients. The DHCP server is the one included in the ISC distribution.

54.5.2. What This Section Covers

This section describes both the client-side components of the ISC and OpenBSD DHCP client and server-side components of the ISC DHCP system. The client-side program, `dhclient`, comes integrated within FreeBSD, and the server-side portion is available from the net/isc-dhcp3-server port. The dhclient(8), dhcp-options(5), and dhclient.conf(5) manual pages, in addition to the references below, are useful resources.

54.5.3. How It Works

When `dhclient`, the DHCP client, is executed on the client machine, it begins broadcasting requests for configuration information. By default, these requests are on UDP port 68. The server replies on UDP 67, giving the client an IP address and other relevant network information such as netmask, router, and DNS servers. All of this information comes in the form of a DHCP "lease" and is only valid for a certain time (configured by the DHCP server maintainer). In this manner, stale IP addresses for clients no longer connected to the network can be automatically reclaimed.

DHCP clients can obtain a great deal of information from the server. An exhaustive list may be found in dhcp-options(5).

54.5.4. FreeBSD Integration

FreeBSD fully integrates the ISC or OpenBSD DHCP client, `dhclient` (according to the FreeBSD version you run). DHCP client support is provided within both the installer and the base system, obviating the need for detailed knowledge of network configurations on any network that runs a DHCP server. `dhclient` has been included in all FreeBSD distributions since 3.2.

DHCP is supported by sysinstall. When configuring a network interface within sysinstall, the second question asked is: "Do you want to try DHCP configuration of the interface?". Answering affirmatively will execute `dhclient`, and if successful, will fill in the network configuration information automatically.

There are two things you must do to have your system use DHCP upon startup:

- Make sure that the bpf device is compiled into your kernel. To do this, add `device bpf` to your kernel configuration file, and rebuild the kernel. For more information about building kernels, see Ρυθμίζοντας τον Πυρήνα του FreeBSD.

  The bpf device is already part of the GENERIC kernel that is supplied with FreeBSD, so if you do not have a custom kernel, you should not need to create one in order to get DHCP working.

For those who are particularly security conscious, you should be warned that bpf is also the device that allows packet sniffers to work correctly (although they still have to be run as `root`). bpf*is* required to use DHCP, but if you are very

sensitive about security, you probably should not add bpf to your kernel in the expectation that at some point in the future you will be using DHCP.

- Edit your /etc/rc.conf to include the following:

```
ifconfig_fxp0="DHCP"
```

Be sure to replace `fxp0` with the designation for the interface that you wish to dynamically configure, as described in Ρυθμίζοντας Τις Κάρτες Δικτύου.

If you are using a different location for `dhclient`, or if you wish to pass additional flags to `dhclient`, also include the following (editing as necessary):

```
dhcp_program="/sbin/dhclient"
dhcp_flags=""
```

The DHCP server, dhcpd, is included as part of the net/isc-dhcp3-server port in the ports collection. This port contains the ISC DHCP server and documentation.

54.5.5. Files

- /etc/dhclient.conf

  `dhclient` requires a configuration file, /etc/dhclient.conf. Typically the file contains only comments, the defaults being reasonably sane. This configuration file is described by the dhclient.conf(5) manual page.

- /sbin/dhclient

  `dhclient` is statically linked and resides in /sbin. The dhclient(8) manual page gives more information about `dhclient`.

- /sbin/dhclient-script

  `dhclient-script` is the FreeBSD-specific DHCP client configuration script. It is described in dhclient-script(8), but should not need any user modification to function properly.

- /var/db/dhclient.leases

  The DHCP client keeps a database of valid leases in this file, which is written as a log. dhclient.leases(5) gives a slightly longer description.

54.5.6. Further Reading

The DHCP protocol is fully described in RFC 2131. An informational resource has also been set up at http://www.dhcp.org/.

54.5.7. Installing and Configuring a DHCP Server

54.5.7.1. What This Section Covers

This section provides information on how to configure a FreeBSD system to act as a DHCP server using the ISC (Internet Software Consortium) implementation of the DHCP server.

The server is not provided as part of FreeBSD, and so you will need to install the net/isc-dhcp3-server port to provide this service. See Εγκατάσταση Εφαρμογών: Πακέτα και Ports for more information on using the Ports Collection.

54.5.7.2. DHCP Server Installation

In order to configure your FreeBSD system as a DHCP server, you will need to ensure that the bpf(4) device is compiled into your kernel. To do this, add `device bpf` to your kernel configuration file, and rebuild the kernel. For more information about building kernels, see Ρυθμίζοντας τον Πυρήνα του FreeBSD.

The bpf device is already part of the GENERIC kernel that is supplied with FreeBSD, so you do not need to create a custom kernel in order to get DHCP working.

Those who are particularly security conscious should note that bpf is also the device that allows packet sniffers to work correctly (although such programs still need privileged access). bpf*is* required to use DHCP, but if you are very sensitive about security, you probably should not include bpf in your kernel purely because you expect to use DHCP at some point in the future.

The next thing that you will need to do is edit the sample dhcpd.conf which was installed by the net/isc-dhcp3-server port. By default, this will be /usr/local/etc/dhcpd.conf.sample, and you should copy this to /usr/local/etc/dhcpd.conf before proceeding to make changes.

54.5.7.3. Configuring the DHCP Server

dhcpd.conf is comprised of declarations regarding subnets and hosts, and is perhaps most easily explained using an example :

```
option domain-name "example.com";①
option domain-name-servers 192.168.4.100;②
option subnet-mask 255.255.255.0;③

default-lease-time 3600;④
max-lease-time 86400;⑤
ddns-update-style none;⑥

subnet 192.168.4.0 netmask 255.255.255.0 {
  range 192.168.4.129 192.168.4.254;⑦
  option routers 192.168.4.1;⑧
}

host mailhost {
```

```
  hardware ethernet 02:03:04:05:06:07;⑨
  fixed-address mailhost.example.com;⑩
}
```

① This option specifies the domain that will be provided to clients as the default search domain. See resolv.conf(5) for more information on what this means.

② This option specifies a comma separated list of DNS servers that the client should use.

③ The netmask that will be provided to clients.

④ A client may request a specific length of time that a lease will be valid. Otherwise the server will assign a lease with this expiry value (in seconds).

⑤ This is the maximum length of time that the server will lease for. Should a client request a longer lease, a lease will be issued, although it will only be valid for `max-lease-time` seconds.

⑥ This option specifies whether the DHCP server should attempt to update DNS when a lease is accepted or released. In the ISC implementation, this option is *required*.

⑦ This denotes which IP addresses should be used in the pool reserved for allocating to clients. IP addresses between, and including, the ones stated are handed out to clients.

⑧ Declares the default gateway that will be provided to clients.

⑨ The hardware MAC address of a host (so that the DHCP server can recognize a host when it makes a request).

⑩ Specifies that the host should always be given the same IP address. Note that using a hostname is correct here, since the DHCP server will resolve the hostname itself before returning the lease information.

Once you have finished writing your dhcpd.conf, you should enable the DHCP server in /etc/rc.conf, i.e. by adding:

```
dhcpd_enable="YES"
dhcpd_ifaces="dc0"
```

Replace the `dc0` interface name with the interface (or interfaces, separated by whitespace) that your DHCP server should listen on for DHCP client requests.

Then, you can proceed to start the server by issuing the following command:

```
# /usr/local/etc/rc.d/isc-dhcpd.sh start
```

Should you need to make changes to the configuration of your server in the future, it is important to note that sending a `SIGHUP` signal to dhcpd does *not* result in the configuration being reloaded, as it does with most daemons. You will need to send a `SIGTERM` signal to stop the process, and then restart it using the command above.

54.5.7.4. Files

- /usr/local/sbin/dhcpd

  dhcpd is statically linked and resides in /usr/local/sbin. The dhcpd(8) manual page installed with the port gives more information about dhcpd.

- /usr/local/etc/dhcpd.conf

  dhcpd requires a configuration file, /usr/local/etc/dhcpd.conf before it will start providing service to clients. This file needs to contain all the information that should be provided to clients that are being serviced, along with information regarding the operation of the server. This configuration file is described by the dhcpd.conf(5) manual page installed by the port.

- /var/db/dhcpd.leases

  The DHCP server keeps a database of leases it has issued in this file, which is written as a log. The manual page dhcpd.leases(5), installed by the port gives a slightly longer description.

- /usr/local/sbin/dhcrelay

  dhcrelay is used in advanced environments where one DHCP server forwards a request from a client to another DHCP server on a separate network. If you require this functionality, then install the net/isc-dhcp3-relay port. The dhcrelay(8) manual page provided with the port contains more detail.

54.6. Domain Name System (DNS)

54.6.1. Overview

FreeBSD utilizes, by default, a version of BIND (Berkeley Internet Name Domain), which is the most common implementation of the DNS protocol. DNS is the protocol through which names are mapped to IP addresses, and vice versa. For example, a query for `www.FreeBSD.org` will receive a reply with the IP address of The FreeBSD Project's web server, whereas, a query for `ftp.FreeBSD.org` will return the IP address of the corresponding FTP machine. Likewise, the opposite can happen. A query for an IP address can resolve its hostname. It is not necessary to run a name server to perform DNS lookups on a system.

FreeBSD currently comes with BIND9 DNS server software by default. Our installation provides enhanced security features, a new file system layout and automated chroot(8) configuration.

DNS is coordinated across the Internet through a somewhat complex system of authoritative root, Top Level Domain (TLD), and other smaller-scale name servers which host and cache individual domain information.

Currently, BIND is maintained by the Internet Software Consortium http://www.isc.org/.

54.6.2. Terminology

To understand this document, some terms related to DNS must be understood.

Term	Definition
Forward DNS	Mapping of hostnames to IP addresses.
Origin	Refers to the domain covered in a particular zone file.
named, BIND, name server	Common names for the BIND name server package within FreeBSD.
Resolver	A system process through which a machine queries a name server for zone information.
Reverse DNS	The opposite of forward DNS; mapping of IP addresses to hostnames.
Root zone	The beginning of the Internet zone hierarchy. All zones fall under the root zone, similar to how all files in a file system fall under the root directory.
Zone	An individual domain, subdomain, or portion of the DNS administered by the same authority.

Examples of zones:

- `.` is the root zone.
- `org.` is a Top Level Domain (TLD) under the root zone.
- `example.org.` is a zone under the `org.` TLD.
- `1.168.192.in-addr.arpa` is a zone referencing all IP addresses which fall under the `192.168.1.*` IP space.

As one can see, the more specific part of a hostname appears to its left. For example, `example.org.` is more specific than `org.`, as `org.` is more specific than the root zone. The layout of each part of a hostname is much like a file system: the /dev directory falls within the root, and so on.

54.6.3. Reasons to Run a Name Server

Name servers usually come in two forms: an authoritative name server, and a caching name server.

An authoritative name server is needed when:

- One wants to serve DNS information to the world, replying authoritatively to queries.
- A domain, such as `example.org`, is registered and IP addresses need to be assigned to hostnames under it.
- An IP address block requires reverse DNS entries (IP to hostname).
- A backup or second name server, called a slave, will reply to queries.

A caching name server is needed when:

- A local DNS server may cache and respond more quickly than querying an outside name server.

When one queries for `www.FreeBSD.org`, the resolver usually queries the uplink ISP's name server, and retrieves the reply. With a local, caching DNS server, the query only has to be made once to the outside world by the caching DNS server. Every additional query will not have to look to the outside of the local network, since the information is cached locally.

54.6.4. How It Works

In FreeBSD, the BIND daemon is called named for obvious reasons.

File	Description
named(8)	The BIND daemon.
rndc(8)	Name server control utility.
/etc/namedb	Directory where BIND zone information resides.
/etc/namedb/named.conf	Configuration file of the daemon.

Depending on how a given zone is configured on the server, the files related to that zone can be found in the master, slave, or dynamic subdirectories of the /etc/namedb directory. These files contain the DNS information that will be given out by the name server in response to queries.

54.6.5. Starting BIND

Since BIND is installed by default, configuring it all is relatively simple.

The default named configuration is that of a basic resolving name server, ran in a chroot(8) environment. To start the server one time with this configuration, use the following command:

```
# /etc/rc.d/named forcestart
```

To ensure the named daemon is started at boot each time, put the following line into the /etc/rc.conf:

```
named_enable="YES"
```

There are obviously many configuration options for /etc/namedb/named.conf that are beyond the scope of this document. However, if you are interested in the startup options for named on FreeBSD, take a look at the `named_*` flags in /etc/defaults/rc.conf and consult the rc.conf(5) manual page. The Χρησιμοποιώντας Το Σύστημα rc Στο FreeBSD section is also a good read.

54.6.6. Configuration Files

Configuration files for named currently reside in /etc/namedb directory and will need modification before use, unless all that is needed is a simple resolver. This is where most of the configuration will be performed.

54.6.6.1. Using `make-localhost`

To configure a master zone for the localhost visit the /etc/namedb directory and run the following command:

```
# sh make-localhost
```

If all went well, a new file should exist in the master subdirectory. The filenames should be localhost.rev for the local domain name and localhost-v6.rev for IPv6 configurations. As the default configuration file, required information will be present in the named.conf file.

54.6.6.2. /etc/namedb/named.conf

```
// $FreeBSD$
//
// Refer to the named.conf(5) and named(8) man pages, and the documentation
// in /usr/shared/doc/bind9 for more details.
//
// If you are going to set up an authoritative server, make sure you
// understand the hairy details of how DNS works.  Even with
// simple mistakes, you can break connectivity for affected parties,
// or cause huge amounts of useless Internet traffic.

options {
    directory   "/etc/namedb";
    pid-file    "/var/run/named/pid";
    dump-file   "/var/dump/named_dump.db";
    statistics-file "/var/stats/named.stats";

// If named is being used only as a local resolver, this is a safe default.
// For named to be accessible to the network, comment this option, specify
// the proper IP address, or delete this option.
    listen-on   { 127.0.0.1; };

// If you have IPv6 enabled on this system, uncomment this option for
// use as a local resolver.  To give access to the network, specify
// an IPv6 address, or the keyword "any".
//  listen-on-v6    { ::1; };

// In addition to the "forwarders" clause, you can force your name
// server to never initiate queries of its own, but always ask its
// forwarders only, by enabling the following line:
//
//  forward only;

// If you've got a DNS server around at your upstream provider, enter
// its IP address here, and enable the line below.  This will make you
// benefit from its cache, thus reduce overall DNS traffic in the Internet.
/*
```

```
    forwarders {
        127.0.0.1;
    };
*/
```

Just as the comment says, to benefit from an uplink's cache, `forwarders` can be enabled here. Under normal circumstances, a name server will recursively query the Internet looking at certain name servers until it finds the answer it is looking for. Having this enabled will have it query the uplink's name server (or name server provided) first, taking advantage of its cache. If the uplink name server in question is a heavily trafficked, fast name server, enabling this may be worthwhile.

`127.0.0.1` will *not* work here. Change this IP address to a name server at your uplink.

```
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below.  Previous versions of BIND always asked
     * questions using port 53, but BIND versions 8 and later
     * use a pseudo-random unprivileged UDP port by default.
     */
     // query-source address * port 53;
};

// If you enable a local name server, don't forget to enter 127.0.0.1
// first in your /etc/resolv.conf so this server will be queried.
// Also, make sure to enable it in /etc/rc.conf.

zone "." {
    type hint;
    file "named.root";
};

zone "0.0.127.IN-ADDR.ARPA" {
    type master;
    file "master/localhost.rev";
};

// RFC 3152
zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA" {
    type master;
    file "master/localhost-v6.rev";
};

// NB: Do not use the IP addresses below, they are faked, and only
// serve demonstration/documentation purposes!
//
// Example slave zone config entries.  It can be convenient to become
// a slave at least for the zone your own domain is in.  Ask
```

```
// your network administrator for the IP address of the responsible
// primary.
//
// Never forget to include the reverse lookup (IN-ADDR.ARPA) zone!
// (This is named after the first bytes of the IP address, in reverse
// order, with ".IN-ADDR.ARPA" appended.)
//
// Before starting to set up a primary zone, make sure you fully
// understand how DNS and BIND works.  There are sometimes
// non-obvious pitfalls.  Setting up a slave zone is simpler.
//
// NB: Don't blindly enable the examples below. :-)  Use actual names
// and addresses instead.

/* An example master zone
zone "example.net" {
    type master;
    file "master/example.net";
};
*/

/* An example dynamic zone
key "exampleorgkey" {
    algorithm hmac-md5;
    secret "sf87HJqjkqh8ac87a02lla==";
};
zone "example.org" {
    type master;
    allow-update {
        key "exampleorgkey";
    };
    file "dynamic/example.org";
};
*/

/* Examples of forward and reverse slave zones
zone "example.com" {
    type slave;
    file "slave/example.com";
    masters {
        192.168.1.1;
    };
};
zone "1.168.192.in-addr.arpa" {
    type slave;
    file "slave/1.168.192.in-addr.arpa";
    masters {
        192.168.1.1;
    };
};
```

```
*/
```

In named.conf, these are examples of slave entries for a forward and reverse zone.

For each new zone served, a new zone entry must be added to named.conf.

For example, the simplest zone entry for `example.org` can look like:

```
zone "example.org" {
    type master;
    file "master/example.org";
};
```

The zone is a master, as indicated by the `type` statement, holding its zone information in /etc/namedb/master/example.org indicated by the `file` statement.

```
zone "example.org" {
    type slave;
    file "slave/example.org";
};
```

In the slave case, the zone information is transferred from the master name server for the particular zone, and saved in the file specified. If and when the master server dies or is unreachable, the slave name server will have the transferred zone information and will be able to serve it.

54.6.6.3. Zone Files

An example master zone file for `example.org` (existing within /etc/namedb/master/example.org) is as follows:

```
$TTL 3600        ; 1 hour
example.org.    IN      SOA      ns1.example.org. admin.example.org. (
                                2006051501      ; Serial
                                10800           ; Refresh
                                3600            ; Retry
                                604800          ; Expire
                                86400           ; Minimum TTL
                        )

; DNS Servers
                IN      NS      ns1.example.org.
                IN      NS      ns2.example.org.

; MX Records
                IN      MX 10   mx.example.org.
                IN      MX 20   mail.example.org.
```

```
                IN      A       192.168.1.1

; Machine Names
localhost       IN      A       127.0.0.1
ns1             IN      A       192.168.1.2
ns2             IN      A       192.168.1.3
mx              IN      A       192.168.1.4
mail            IN      A       192.168.1.5

; Aliases
www             IN      CNAME   @
```

Note that every hostname ending in a "." is an exact hostname, whereas everything without a trailing "." is referenced to the origin. For example, `www` is translated into `www.origin`. In our fictitious zone file, our origin is `example.org.`, so `www` would translate to `www.example.org.`

The format of a zone file follows:

```
recordname      IN recordtype   value
```

The most commonly used DNS records:

SOA

start of zone authority

NS

an authoritative name server

A

a host address

CNAME

the canonical name for an alias

MX

mail exchanger

PTR

a domain name pointer (used in reverse DNS)

```
example.org. IN SOA ns1.example.org. admin.example.org. (
                        2006051501      ; Serial
                        10800           ; Refresh after 3 hours
                        3600            ; Retry after 1 hour
                        604800          ; Expire after 1 week
                        86400 )         ; Minimum TTL of 1 day
```

`example.org.`

the domain name, also the origin for this zone file.

`ns1.example.org.`

the primary/authoritative name server for this zone.

`admin.example.org.`

the responsible person for this zone, email address with "@" replaced. (admin@example.org becomes `admin.example.org`)

`2006051501`

the serial number of the file. This must be incremented each time the zone file is modified. Nowadays, many admins prefer a `yyyymmddrr` format for the serial number. `2006051501` would mean last modified 05/15/2006, the latter `01` being the first time the zone file has been modified this day. The serial number is important as it alerts slave name servers for a zone when it is updated.

```
       IN NS           ns1.example.org.
```

This is an NS entry. Every name server that is going to reply authoritatively for the zone must have one of these entries.

```
localhost       IN      A       127.0.0.1
ns1             IN      A       192.168.1.2
ns2             IN      A       192.168.1.3
mx              IN      A       192.168.1.4
mail            IN      A       192.168.1.5
```

The A record indicates machine names. As seen above, `ns1.example.org` would resolve to `192.168.1.2`.

```
                IN      A       192.168.1.1
```

This line assigns IP address `192.168.1.1` to the current origin, in this case `example.org`.

```
www             IN CNAME        @
```

The canonical name record is usually used for giving aliases to a machine. In the example, `www` is aliased to the "master" machine which name equals to domain name `example.org` (`192.168.1.1`). CNAMEs can be used to provide alias hostnames, or round robin one hostname among multiple machines.

```
              IN MX   10      mail.example.org.
```

The MX record indicates which mail servers are responsible for handling incoming mail for the zone. `mail.example.org` is the hostname of the mail server, and 10 being the priority of that mail server.

One can have several mail servers, with priorities of 10, 20 and so on. A mail server attempting to deliver to `example.org` would first try the highest priority MX (the record with the lowest priority number), then the second highest, etc, until the mail can be properly delivered.

For in-addr.arpa zone files (reverse DNS), the same format is used, except with PTR entries instead of A or CNAME.

```
$TTL 3600

1.168.192.in-addr.arpa. IN SOA ns1.example.org. admin.example.org. (
                        2006051501      ; Serial
                        10800           ; Refresh
                        3600            ; Retry
                        604800          ; Expire
                        3600 )          ; Minimum

        IN      NS      ns1.example.org.
        IN      NS      ns2.example.org.

1       IN      PTR     example.org.
2       IN      PTR     ns1.example.org.
3       IN      PTR     ns2.example.org.
4       IN      PTR     mx.example.org.
5       IN      PTR     mail.example.org.
```

This file gives the proper IP address to hostname mappings of our above fictitious domain.

54.6.7. Caching Name Server

A caching name server is a name server that is not authoritative for any zones. It simply asks queries of its own, and remembers them for later use. To set one up, just configure the name server as usual, omitting any inclusions of zones.

54.6.8. Security

Although BIND is the most common implementation of DNS, there is always the issue of security. Possible and exploitable security holes are sometimes found.

While FreeBSD automatically drops named into a chroot(8) environment; there are several other security mechanisms in place which could help to lure off possible DNS service attacks.

It is always good idea to read CERT's security advisories and to subscribe to the ηλεκτρονική λίστα Ανακοινώσεων για Θέματα Ασφάλειας του FreeBSD to stay up to date with the current Internet and FreeBSD security issues.

If a problem arises, keeping sources up to date and having a fresh build of named would not hurt.

54.6.9. Further Reading

BIND/named manual pages: rndc(8) named(8) named.conf(8)

- Official ISC BIND Page
- Official ISC BIND Forum
- BIND FAQ
- O'Reilly DNS and BIND 5th Edition
- RFC1034 - Domain Names - Concepts and Facilities
- RFC1035 - Domain Names - Implementation and Specification

54.7. Ο εξυπηρετητής HTTP Apache

54.7.1. Σύνοψη

Το FreeBSD χρησιμοποιείται για να φιλοξενεί παγκοσμίως ιστοσελίδες μεγάλης επισκεψιμότητας. Οι περισσότεροι διακομιστές web στο διαδίκτυο χρησιμοποιούν τον εξυπηρετητή HTTP Apache. Τα πακέτα λογισμικού του Apache θα πρέπει να περιέχονται στο μέσο εγκατατάστασης του FreeBSD που χρησιμοποιείτε. Αν δεν εγκαταστήσατε τον Apache κατά την διάρκεια της εγκατάστασης του FreeBSD, τότε μπορείτε να τον εγκαταστήσετε από το πακέτο www/apache13 ή από το πακέτο www/apache20.

Αφού ολοκληρώσετε επιτυχώς την εγκατάσταση του Apache, θα πρέπει να κάνετε τις απαραίτητες ρυθμίσεις.

Αυτή η ενότητα καλύπτει την έκδοση εξυπηρετητών Apache HTTP 1.3.X, μιας που αυτή η έκδοση είναι η πιο διαδεδομένη για το FreeBSD. Ο Apache 2.X παρουσιάζει πολλές νέες τεχνολογίες αλλά αυτές δεν περιγράφονται σε αυτή την ενότητα. Περισσότερες πληροφορίες για τον Apache 2.X, μπορείτε να δείτε στην σελίδα http://httpd.apache.org/.

54.7.2. Ρυθμίσεις

Στο FreeBSD το σημαντικότερο αρχείο ρυθμίσεων του Εξυπηρετητή HTTP Apache είναι το /usr/local/etc/apache/httpd.conf. Είναι ένα τυπικό UNIX® ρυθμιστικό αρχείο κειμένου, με γραμμές σχολίων που ξεκινούν με τον χαρακτήρα #. Σκοπός μας εδώ δεν είναι μια ολοκληρωμένη περιγραφή όλων των πιθανών επιλογών, επομένως θα περιγράψουμε μόνο τις πιο δημοφιλείς επιλογές ρυθμίσεις (configuration directives).

`ServerRoot "/usr/local"`

Εδώ περιγράφεται ο προεπιλεγμένος ιεραρχικά κατάλογος εγκατάστασης για τον Apache. Τα εκτελέσιμα αρχεία είναι αποθηκευμένα στους υποκαταλόγους bin και sbin του καταλόγου

"ServerRoot" και τα αρχεία ρυθμίσεων αποθηκεύονται στον κατάλογο etc/apache.

`ServerAdmin you@your.address`

Η ηλεκτρονική διεύθυνση στην οποία θα πρέπει να αποστέλλονται αναφορές προβλημάτων σχετικά με τον εξυπηρετητή. Αυτή η διεύθυνση εμφανίζεται σε κάποιες σελίδες που δημιουργούνται από τον εξυπηρετητή, όπως οι σελίδες σφαλμάτων.

`ServerName www.example.com`

Το `ServerName` σας επιτρέπει να θέσετε ένα όνομα κόμβου (hostname) για τον εξυπηρετητή σας, το οποίο αποστέλλεται πίσω στους clients αν είναι διαφορετικό από εκείνο που έχετε ήδη ρυθμίσει στον κόμβο σας (εδώ μπορείτε, για παράδειγμα, να χρησιμοποιήσετε `www` αντί του πραγματικού ονόματος του κόμβου).

`DocumentRoot "/usr/local/www/data"`

`DocumentRoot`: Είναι ο κατάλογος από τον οποίο θα προσφέρονται τα έγγραφα σας. Προεπιλεγμένα, όλα τα αιτήματα θα εξυπηρετούνται από αυτό τον κατάλογο, αλλά μπορούν επίσης να χρησιμοποιηθούν συμβολικοί δεσμοί (symbolic link) ή παρωνύμια (aliases) που θα στοχεύουν σε άλλες τοποθεσίες.

Πριν κάνετε οποιαδήποτε αλλαγή, είναι καλό να δημιουργείτε αντίγραφα ασφαλείας (backup) του αρχείου ρυθμίσεων του Apache. Μόλις κρίνετε πως είστε ικανοποιημένος με τις αρχικές ρυθμίσεις μπορείτε να ξεκινήσετε με την εκτέλεση του Apache.

54.7.3. Εκτέλεση του Apache

Ο Apache δεν τρέχει διαμέσου του υπερ-διακομιστή inetd όπως κάνουν πολλοί άλλοι δικτυακοί εξυπηρετητές. Είναι ρυθμισμένος να τρέχει αυτόνομα για να εξυπηρετεί καλύτερα τις αιτήσεις HTTP των πελατών του, δηλαδή των προγραμμάτων πλοήγησης (browsers). Η εγκατάσταση του Apache από τα FreeBSD Ports περιέχει ένα βοηθητικό shell script για την εκκίνηση, το σταμάτημα και την επανεκκίνηση του εξυπηρετητή. Για να ξεκινήσετε τον Apache για πρώτη φορά, απλά τρέξτε:

```
# /usr/local/sbin/apachectl start
```

Μπορείτε οποιαδήποτε στιγμή να σταματήσετε τον εξυπηρετητή, πληκτρολογώντας:

```
# /usr/local/sbin/apachectl stop
```

Μετά από αλλαγές που πιθανώς να κάνατε για οποιονδήποτε λόγο στο αρχείο ρυθμίσεων, θα χρειαστεί να επανεκκινήσετε τον εξυπηρετητή:

```
# /usr/local/sbin/apachectl restart
```

Για να επανεκκινήσετε τον Apache δίχως να διακόψετε τις τρέχουσες συνδέσεις, τρέξτε:

```
# /usr/local/sbin/apachectl graceful
```

Περισσότερες πληροφορίες θα βρείτε στη σελίδα βοήθειας του apachectl(8).

Για να ξεκινάει ο Apache αυτόματα κατά τη διάρκεια εκκίνησης του συστήματος, προσθέστε την ακόλουθη γραμμή στο /etc/rc.conf:

```
apache_enable="YES"
```

Αν επιθυμείτε να παρέχονται κατά την εκκίνηση του συστήματος πρόσθετες επιλογές στην γραμμή εντολών για το πρόγραμμα Apache `httpd` μπορείτε να τις δηλώσετε με μια πρόσθετη γραμμή στο rc.conf:

```
apache_flags=""
```

Τώρα που έχει ξεκινήσει ο εξυπηρετής web, μπορείτε να δείτε την ιστοσελίδα σας στοχεύοντας το πρόγραμμα πλοήγησης στο `http://localhost/`. Η προκαθορισμένη σελίδα που εμφανίζεται είναι η /usr/local/www/data/index.html.

54.7.4. Virtual Hosting

Ο Apache υποστηρίζει δύο διαφορετικούς τύπους Virtual Hosting. Το Ονομαστικό virtual hosting χρησιμοποιεί τους HTTP/1.1 headers για να καθορίσει τον κόμβο. Αυτό επιτρέπει την κοινή χρήση της ίδιας IP για πολλά και διαφορετικά domains.

Για να ρυθμίσετε τον Apache να χρησιμοποιεί το Ονομαστικό Virtual Hosting εισάγετε μια καταχώριση στο httpd.conf σαν την ακόλουθη:

```
NameVirtualHost *
```

Αν ο διακομιστής web ονομάζεται `www.domain.tld` και επιθυμείτε να εγκαταστήσετε ένα virtual domain για το `www.someotherdomain.tld` τότε θα πρέπει να προσθέσετε τις ακόλουθες καταχωρήσεις στο httpd.conf:

```
<VirtualHost *>
ServerName www.domain.tld
DocumentRoot /www/domain.tld
</VirtualHost>

<VirtualHost *>
ServerName www.someotherdomain.tld
DocumentRoot /www/someotherdomain.tld
</VirtualHost>
```

Αντικαταστήστε τις παραπάνω διευθύνσεις με εκείνες που επιθυμείτε να χρησιμοποιήσετε και την κατάλληλη διαδρομή προς τα έγγραφά σας.

Για περισσότερες πληροφορίες σχετικά με τις ρυθμίσεις για τα virtual host, σας προτρέπουμε να συμβουλευτείτε την επίσημη τεκμηρίωση του Apache στο http://httpd.apache.org/docs/vhosts/.

54.7.5. Apache Modules

Υπάρχουν πολλοί και διάφοροι διαθέσιμοι τύποι αρθρωμάτων (modules) για τον Apache, τα οποία επεκτείνουν κι εμπλουτίζουν τις λειτουργίες του βασικού εξυπηρετητή. Η Συλλογή των Ports του FreeBSD παρέχει έναν εύκολο τρόπο για να εγκαταστήσετε τον Apache και μερικά από τα πιο δημοφιλή αρθρώματα.

54.7.5.1. mod_ssl

Το άρθρωμα mod_ssl χρησιμοποιεί την βιβλιοθήκη OpenSSL για να παρέχει ισχυρή κρυπτογράφηση διαμέσου των πρωτοκόλων Secure Sockets Layer (SSL v2/v3) και Transport Layer Security (TLS v1). Το άρθρωμα παρέχει όλα τα απαραίτητα συστατικά για να μπορεί να αιτείται υπογεγγραμμένα πιστοποιητικά από έμπιστους εξουσιοδοτημένους φορείς πιστοποίησης έτσι ώστε να μπορείτε να τρέχετε έναν ασφαλή εξυπηρετητή web στο FreeBSD.

Εάν δεν έχετε εγκαταστήσει ακόμη τον Apache, μπορείτε να εγκαταστήσετε την έκδοση του Apache 1.3.X που περιλαμβάνει το mod_ssl από την port www/apache13-modssl . Το SSL είναι επίσης διαθέσιμο για τον Apache 2.X στην port www/apache20, όπου το SSL είναι ενεργοποιημένο από προεπιλογή.

54.7.5.2. Δυναμικές Ιστοσελίδες με Perl & PHP

Την τελευταία δεκαετία, πολλές επιχειρήσεις στρέψανε τις δραστηριότητες τους προς το Ίντερνετ με σκοπό να βελτιώσουν τα έσοδα τους και για μεγαλύτερη προβολή. Αυτό με τη σειρά του δημιούργησε την ανάγκη για διαδραστικό διαδικτυακό περιεχόμενο. Ενώ κάποιες εταιρείες, όπως η Microsoft®, παρουσίασαν λύσεις ενσωματωμένες στα ιδιόκτητα προϊόντα τους, η κοινότητα ανοιχτού λογισμικού έλαβε το μήνυμα. Στις σύγχρονες επιλογές για διαδικτυακές σελίδες δυναμικού περιεχομένου περιλαμβάνονται τα Django, Ruby on Rails, mod_perl και mod_php. mod_perl & mod_php.

54.7.5.2.1. mod_perl

Το γεγονός συνύπαρξης Apache/Perl φέρνει κοντά τη μεγάλη δύναμη της γλώσσας προγραμματισμού Perl και τον εξυπηρετητή HTTP Apache. Με το άρθρωμα mod_perl έχετε τη δυνατότητα να γράψετε επεκτάσεις για τον Apache εξ' ολοκλήρου σε Perl. Επιπλέον, ο διατηρήσιμος μεταγλωττιστής που είναι ενσωματωμένος στον εξυπηρετητή σας επιτρέπει να αποφύγετε την χρήση ενός εξωτερικού μεταγλωττιστή Perl και να επιβαρυνθείτε από το χρόνο εκκίνησης του.

Το mod_perl διατίθεται με διάφορους τρόπους. Για να χρησιμοποιήσετε το mod_perl να θυμάστε ότι το mod_perl 1.0 mod_perl 1.0 δουλεύει μόνο με τον Apache 1.3 και το mod_perl 2.0 δουλεύει μόνο με τον Apache 2. Το mod_perl 1.0 είναι διαθέσιμο στο port www/mod_perl ενώ μια στατικά μεταγλωττισμένη έκδοση είναι διαθέσιμη στο www/apache13-modperl. Το mod_perl 2.0 διατίθεται στο port www/mod_perl2.

54.7.5.2.2. mod_php

Το PHP, γνωστό και ως "PHP: Hypertext Preprocessor" είναι μια script γλώσσα προγραμματισμού γενικής χρήσης αλλά ιδιαίτερα κατάλληλη για ανάπτυξη λογισμικού Web. Η σύνταξή της προέρχεται από τις C, Java™ και Perl και έχει την δυνατότητα να ενσωματώνεται σε κώδικα HTML, με σκοπό να επιτρέπει στους προγραμματιστές web να γράφουν γρήγορα δυναμικές ιστοσελίδες.

Ο Apache υποστηρίζει το PHP5. Μπορείτε να ξεκινήσετε εγκαθιστώντας το πακέτο lang/php5.

Αν το πακέτο lang/php5 εγκαθίσταται για πρώτη φορά, αυτόματα θα σας εμφανιστούν όλες οι δυνατές επιλογές `OPTIONS`. Αν κάποιο μενού δεν εμφανίζεται, π.χ. επειδή το πακέτο lang/php5 είχε εγκατασταθεί στο παρελθόν, μπορείτε πάντα να ρυθμίσετε από την αρχή το πακέτο, τρέχοντας στον κατάλογο του port:

```
# make config
```

Στις επιλογές εγκατάστασης, διαλέξτε την επιλογή `APACHE` ώστε να συμπεριληφθεί και το άρθρωμα mod_php για τον εξυπηρετητή Apache.

Μερικές τοποθεσίες χρησιμοποιούν ακόμη το PHP4 για διάφορους λόγους (π.χ. θέματα συμβατότητος ή επειδή έχουν ήδη εγκατεστημένες εφαρμογές που το απαιτούν). Αν είναι ανάγκη να χρησιμοποιήσετε το mod_php4 αντί του mod_php5, τότε χρησιμοποιείστε το port lang/php4. Το port lang/php4 υποστηρίζει πολλές από τις ρυθμίσεις και τις επιλογές εγκατάστασης του port lang/php5.

Με αυτό τον τρόπο θα εγκατασταθούν και θα ρυθμιστούν τα απαιτούμενα αρθρώματα ώστε να υποστηρίζουν δυναμικές εφαρμογές PHP. Για επιβεβαίωση ελέγξτε πως έχουν προστεθεί στις αντίστοιχες ενότητες του /usr/local/etc/apache/httpd.conf τα ακόλουθα

```
LoadModule php5_module        libexec/apache/libphp5.so
```

```
AddModule mod_php5.c
    <IfModule mod_php5.c>
        DirectoryIndex index.php index.html
    </IfModule>
    <IfModule mod_php5.c>
        AddType application/x-httpd-php .php
        AddType application/x-httpd-php-source .phps
    </IfModule>
```

Αφού ολοκληρώσετε τον έλεγχο, για να φορτωθεί το άρθρωμα PHP χρειάζεται μια απλή κλήση με την εντολή `apachectl` για μια κανονική (graceful) επανεκκίνηση:

```
# apachectl graceful
```

Για μελλοντικές αναβαθμίσεις του PHP, δεν απαιτείται η εντολή `make config`. Οι επιλεγμένες `OPTIONS` αποθηκεύονται αυτόματα από το μηχανισμό εγκατάστασης των Ports του FreeBSD.

Η σύνθεση του PHP στο FreeBSD, είναι εξαιρετικά στοιχειακή, και ο βασικός κορμός που έχει εγκατασταθεί είναι πολύ περιορισμένος. Είναι πολύ εύκολο όμως να προσθέσουμε επεκτάσεις χρησιμοποιώντας το port lang/php5-extensions. Αυτό το port παρέχει μενού επιλογών για την εγκατάσταση των επεκτάσιμων συστατικών του PHP. Εναλλακτικά, μπορείτε να εγκαταστήσετε καθεμία επέκταση ξεχωριστά χρησιμοποιώντας το κατάλληλο port.

Για παράδειγμα, για να προσθέσετε στο PHP5, τη δυνατότητα υποστήριξης για βάσεις δεδομένωνMySQL απλά εγκαταστήστε το port databases/php5-mysql.

Μετά την εγκατάσταση ενός νέου αρθρώματος ή κάποιας άλλης επέκτασης, ο εξυπηρετητής Apache θα πρέπει να επαναφορτωθεί για να ενεργοποιηθούν οι νέες ρυθμίσεις:

```
# apachectl graceful
```

54.8. Πρωτόκολο Μεταφοράς Αρχείων (FTP)

54.8.1. Σύνοψη

Το Πρωτόκολο Μεταφοράς Αρχείων (File Transfer Protocol - FTP) παρέχει στους χρήστες έναν εύκολο τρόπο για να μεταφέρουν τα αρχεία τους από και προς έναν εξυπηρετητή FTP. Το βασικό σύστημα του FreeBSD περιλαμβάνει ένα εξυπηρετητή FTP, το ftpd. Αυτό καθιστά την εγκατάσταση και την διαχείριση του εξυπηρετητή FTP πολύ εύκολη υπόθεση.

54.8.2. Ρυθμίσεις

Το πιο σημαντικό βήμα στις ρυθμίσεις είναι να αποφασίσετε σε ποιούς λογαριασμούς θα επιτραπεί η πρόσβαση στον εξυπηρετητή FTP. Ένα συνηθισμένο σύστημα FreeBSD δημιουργεί μερικούς λογαριασμούς συστήματος για διάφορους δαίμονες, αλλά δεν πρέπει να επιτρέπεται η πρόσβαση στο σύστημα με αυτούς τους λογαριασμούς. Το αρχείο /etc/ftpusers περιέχει μια λίστα από χρήστες για τους οποίους απορρίπτεται η πρόσβαση μέσω FTP. Προεπιλεγμένα, περιέχονται οι προαναφερθέντες λογαριασμοί του συστήματος, αλλά μπορείτε επίσης να προσθέσετε συγκεκριμένους χρήστες που δε θα πρέπει να έχουν πρόσβαση μέσω FTP.

Μπορείτε αν θέλετε να περιορίσετε την πρόσβαση σε κάποιους χρήστες, δίχως όμως να τους εμποδίσετε πλήρως. Αυτό μπορεί να συμβεί με τις ρυθμίσεις του αρχείου /etc/ftpchroot. Αυτό το αρχείο περιέχει λίστες χρηστών και ομάδων περιορισμένης πρόσβασης FTP. Η σελίδα βοήθειας ftpchroot(5) περιέχει όλες τις απαραίτητες λεπτομέρειες, επομένως δε θα χρειαστεί να μπούμε σε λεπτομέρειες εδώ.

Αν επιθυμείτε να ενεργοποιήσετε ανώνυμη πρόσβαση FTP στον εξυπηρετητή σας, θα πρέπει να δημιουργήσετε, στο FreeBSD σύστημα σας, ένα χρήστη με όνομα `ftp` . Οι ανώνυμοι χρήστες θα μπορούν να εισέρχονται στον εξυπηρετητή FTP με το γενικό όνομα χρήστη `ftp` ή με `anonymous` και με οποιαδήποτε κωδικό πρόσβασης (συνηθίζεται να ζητείται η διεύθυνση email του χρήστη ως κωδικός πρόσβασης). Ο εξυπηρετητής FTP θα καλέσει το chroot(2) μόλις εισέλθη ο ανώνυμος χρήστης, για να

του περιορίσει την πρόσβαση, επιτρέποντας του μόνο τον αρχικό κατάλογο (home directory) του χρήστη `ftp`.

Υπάρχουν δύο αρχεία κειμένου για τον ορισμό μηνυμάτων καλωσορίσματος που θα εμφανίζονται στους πελάτες FTP. Το περιεχόμενο του αρχείου /etc/ftpwelcome εμφανίζεται στους χρήστες πριν φτάσουν στην προτροπή εισόδου. Μετά από μια πετυχημένη είσοδο στο σύστημα, εμφανίζεται το περιεχόμενο του αρχείου /etc/ftpmotd. Παρατηρήστε πως η διαδρομή σε αυτό το αρχείο είναι σχετική με το περιβάλλον πρόσβασης, επομένως για τους ανώνυμους χρήστες θα εμφανίζεται το περιεχόμενο του αρχείου ~ftp/etc/ftpmotd.

Αφού ρυθμίσετε κατάλληλα τον εξυπηρετητή FTP, θα πρέπει να τον ενεργοποιήσετε στο αρχείο /etc/inetd.conf. Το μόνο που χρειάζεται να κάνετε είναι να αφαιρέσετε το σύμβολο σχολιασμού "#" μπροστά από την υπάρχουσα γραμμή ftpd :

```
ftp stream  tcp nowait  root    /usr/libexec/ftpd   ftpd -l
```

Όπως εξηγήσαμε στο Reloading the inetd configuration file, η διεργασία inetd θα πρέπει να ξαναφορτώνεται αν έχουν γίνει αλλαγές στο αρχείο ρυθμίσεων της.

Τώρα μπορείτε να δώσετε τα στοιχεία του λογαριασμού σας για να εισέλθετε στον εξυπηρετητή FTP.

```
% ftp localhost
```

54.8.3. Συντήρηση

Ο δαίμονας ftpd χρησιμοποιεί το syslog(3) για την δημιουργία μηνυμάτων αναφοράς. Προεπιλεγμένα, ο δαίμονας των log του συστήματος θα εναποθέτει τις σχετικές με το FTP αναφορές στο αρχείο /var/log/xferlog. Η τοποθεσία του αρχείου αναφοράς μπορεί να τροποποιηθεί αλλάζοντας την ακόλουθη γραμμή στο /etc/syslog.conf:

```
ftp.info      /var/log/xferlog
```

Πρέπει να είστε ενήμεροι για τα προβλήματα που μπορούν να παρουσιαστούν σχετικά με τη λειτουργία ενός ανώνυμου εξυπηρετητή FTP. Ειδικότερα, θα πρέπει να σκεφτείτε σοβαρά αν όντως επιθυμείτε να έχουν δυνατότητα να ανεβάζουν αρχεία οι ανώνυμοι χρήστες σας. Αν αφήσετε οποιονδήποτε ανώνυμο χρήστη να ανεβάζει αρχεία, μπορεί ξαφνικά να ανακαλύψετε πως ο εξυπηρετητής σας FTP χρησιμοποιείται για διακίνηση πειρατικού εμπορικού λογισμικού ή για άλλο, ακόμα χειρότερο, παράνομο υλικό. Εάν όντως χρειάζεται οι χρήστες να έχουν άδεια προσθήκης αρχείων, τότε θα πρέπει να ρυθμίσετε τις άδειες έτσι ώστε τα αρχεία αυτά να μην είναι ορατά από άλλους ανώνυμους χρήστες, έως ότου να πάρουν την ασφαλή έγκριση σας.

54.9. File and Print Services for Microsoft® Windows® clients (Samba)

54.9.1. Overview

Samba is a popular open source software package that provides file and print services for Microsoft® Windows® clients. Such clients can connect to and use FreeBSD filespace as if it was a local disk drive, or FreeBSD printers as if they were local printers.

Samba software packages should be included on your FreeBSD installation media. If you did not install Samba when you first installed FreeBSD, then you can install it from the net/samba3 port or package.

54.9.2. Configuration

A default Samba configuration file is installed as /usr/local/etc/smb.conf.default. This file must be copied to /usr/local/etc/smb.conf and customized before Samba can be used.

The smb.conf file contains runtime configuration information for Samba, such as definitions of the printers and "file system shares" that you would like to share with Windows® clients. The Samba package includes a web based tool called swat which provides a simple way of configuring the smb.conf file.

54.9.2.1. Using the Samba Web Administration Tool (SWAT)

The Samba Web Administration Tool (SWAT) runs as a daemon from inetd. Therefore, the following line in /etc/inetd.conf should be uncommented before swat can be used to configure Samba:

```
swat   stream  tcp     nowait/400      root    /usr/local/sbin/swat
```

As explained in Reloading the inetd configuration file, the inetd must be reloaded after this configuration file is changed.

Once swat has been enabled in inetd.conf, you can use a browser to connect to http://localhost:901. You will first have to log on with the system `root` account.

Once you have successfully logged on to the main Samba configuration page, you can browse the system documentation, or begin by clicking on the **Globals** tab. The **Globals** section corresponds to the variables that are set in the `[global]` section of /usr/local/etc/smb.conf.

54.9.2.2. Global Settings

Whether you are using swat or editing /usr/local/etc/smb.conf directly, the first directives you are likely to encounter when configuring Samba are:

`workgroup`

NT Domain-Name or Workgroup-Name for the computers that will be accessing this server.

`netbios name`

This sets the NetBIOS name by which a Samba server is known. By default it is the same as the first component of the host's DNS name.

`server string`

This sets the string that will be displayed with the `net view` command and some other networking tools that seek to display descriptive text about the server.

54.9.2.3. Security Settings

Two of the most important settings in /usr/local/etc/smb.conf are the security model chosen, and the backend password format for client users. The following directives control these options:

`security`

The two most common options here are `security = share` and `security = user`. If your clients use usernames that are the same as their usernames on your FreeBSD machine then you will want to use user level security. This is the default security policy and it requires clients to first log on before they can access shared resources.

In share level security, client do not need to log onto the server with a valid username and password before attempting to connect to a shared resource. This was the default security model for older versions of Samba.

`passdb backend`

Samba has several different backend authentication models. You can authenticate clients with LDAP, NIS+, a SQL database, or a modified password file. The default authentication method is `smbpasswd`, and that is all that will be covered here.

Assuming that the default `smbpasswd` backend is used, the /usr/local/private/smbpasswd file must be created to allow Samba to authenticate clients. If you would like to give your UNIX® user accounts access from Windows® clients, use the following command:

```
# smbpasswd -a username
```

Please see the Official Samba HOWTO for additional information about configuration options. With the basics outlined here, you should have everything you need to start running Samba.

54.9.3. Starting Samba

The net/samba3 port adds a new startup script, which can be used to control Samba. To enable this script, so that it can be used for example to start, stop or restart Samba, add the following line to the /etc/rc.conf file:

```
samba_enable="YES"
```

This will also configure Samba to automatically start at system boot time.

It is possible then to start Samba at any time by typing:

```
# /usr/local/etc/rc.d/samba start
```

```
Starting SAMBA: removing stale tdbs :
Starting nmbd.
Starting smbd.
```

Please refer to Χρησιμοποιώντας Το Σύστημα rc Στο FreeBSD for more information about using rc scripts.

Samba actually consists of three separate daemons. You should see that both the nmbd and smbd daemons are started by the samba.sh script. If you enabled winbind name resolution services in smb.conf, then you will also see that the winbindd daemon is started.

You can stop Samba at any time by typing :

```
# /usr/local/etc/rc.d/samba.sh stop
```

Samba is a complex software suite with functionality that allows broad integration with Microsoft® Windows® networks. For more information about functionality beyond the basic installation described here, please see http://www.samba.org.

54.10. Συγχρονισμός Ρολογιού Συστήματος με NTP

54.10.1. Σύνοψη

Με το πέρασμα του χρόνου, το ρολόι συστήματος ενός υπολογιστή έχει την τάση να αποσυγχρονίζεται. Το Πρωτόκολο Χρονισμού Δικτύων (Network Time Protocol ή NTP) παρέχει ένα τρόπο για να εξασφαλίσετε την ακρίβεια του clock σας.

Πολλές διαδικτυακές υπηρεσίες βασίζονται ή ωφελούνται σε μεγάλο βαθμό από την ακρίβεια του ρολογιού συστήματος ενός υπολογιστή. Για παράδειγμα, ένας εξυπηρετητής web μπορεί να δεχθεί αιτήσεις για αποστολή ενός αρχείου όταν το αρχείο αυτό έχει τροποποιηθεί μέχρι κάποια συγκεκριμένη ώρα. Σε ένα περιβάλλον τοπικού δικτύου, είναι θεμελιώδης αρχή οι υπολογιστές που θα διαμοιραστούν αρχεία από τον ίδιο διακομιστή αρχείων να έχουν συγχρονισμένα ρολόγια, έτσι ώστε τα χρονικά χαρακτηριστικά του αρχείου να συμφωνούν. Επίσης διεργασίες όπως η cron(8) βασίζονται σε ένα ακριβές ρολόι ώστε να μπορούν να τρέχουν εντολές στους προκαθορισμένους χρόνους.

Το FreeBSD διατίθεται με τον εξυπηρετητή NTP ntpd(8), ο οποίος μπορεί να χρησιμοποιηθεί για να συγχρονίζει το ρολόι συστήματος του υπολογιστή σας, εξετάζοντας άλλους εξυπηρετητές NTP ή να παρέχει ο ίδιος υπηρεσίες συγχρονισμού σε άλλα μηχανήματα.

54.10.2. Επιλογή των Κατάλληλων Εξυπηρετητών NTP

Για να συγχρονίσετε το ρολόι συστήματος του υπολογιστή σας θα πρέπει να βρείτε έναν ή περισσότερους διαθέσιμους NTP εξυπηρετητές για να χρησιμοποιήσετε. Ο διαχειριστής δικτύου ή ο ISP σας μπορεί να έχουν εγκαταστήσει κάποιον εξυπηρετητή NTP για αυτό το σκοπό - ελέγξτε την τεκμηρίωση τους να δείτε αν υπάρχει τέτοια περίπτωση. Επιπλέον, υπάρχει μία online λίστα εξυπηρετητών δημόσιας πρόσβασης, που μπορείτε να χρησιμοποιήσετε για να βρείτε έναν κοντινό

εξυπηρετητή NTP. Όποιον εξυπηρετητή κι αν επιλέξετε, ενημερωθείτε για την πολιτική χρήσης του και ζητήστε άδεια να τον χρησιμοποιήσετε αν χρειάζεται τέτοια άδεια.

Είναι καλή ιδέα να επιλέξετε πολλούς εξυπηρετητές NTP, οι οποίοι να μην συνδέονται μεταξύ τους, στην περίπτωση που κάποιος από τους εξυπηρετητές που χρησιμοποιείτε γίνει απρόσιτος ή το ρολόι του είναι ανακριβές. Ο εξυπηρετητής ntpd(8) του FreeBSD χειρίζεται έξυπνα τις απαντήσεις που λαμβάνει από τους υπόλοιπους εξυπηρετητές - ευνοεί τους πιο αξιόπιστους και δείχνει μικρότερη προτίμηση στους λιγότερο αξιόπιστους εξυπηρετητές.

54.10.3. Ρυθμίστε Το Μηχάνημα Σας

54.10.3.1. Βασικές Ρυθμίσεις

Αν επιθυμείτε να συγχρονίζεται το clock σας μόνο κατά την εκκίνηση λειτουργίας του μηχανήματος, τότε μπορείτε να χρησιμοποιήσετε το ntpdate(8). Αυτός ο τρόπος συγχρονισμού είναι κατάλληλος για μηχανήματα desktop τα οποία κάνουν επανακκίνηση ανά τακτά χρονικά διαστήματα και μόνο σε ειδικές περιπτώσεις έχουν ανάγκη συγχρονισμού. Αντιθέτως, τα υπόλοιπα μηχανήματα θα πρέπει να τρέχουν την διεργασία ntpd(8).

Είναι καλή πρακτική τα μηχανήματα που τρέχουν ntpd(8) να χρησιμοποιούν και το ntpdate(8) κατά τη διάρκεια εκκίνησης τους. Το ntpd(8) μεταβάλλει το clock βαθμιαία, ενώ το ntpdate(8) ρυθμίζει άμεσα το clock ανεξάρτητα από το πόσο μεγάλη είναι η χρονική διαφορά μεταξύ πραγματικής και τρέχουσας ώρας του clock του μηχανήματος.

Για να ενεργοποιήσετε το ntpdate(8) κατά την εκκίνηση, προσθέστε `ntpdate_enable="YES"` στο /etc/rc.conf. Θα πρέπει να προσδιορίσετε στο `ntpdate_flags` όλους τους διακομιστές με τους οποίους επιθυμείτε να συγχρονίζεστε και όλα τα flag που θέλετε να συνοδεύουν τοntpdate(8).

54.10.3.2. Γενικές Ρυθμίσεις

Οι ρυθμίσεις του NTP βρίσκονται στο αρχείο /etc/ntp.conf και είναι στη μορφή που περιγράφεται στο ntp.conf(5). Ακολουθεί ένα απλό παράδειγμα:

```
server ntplocal.example.com prefer
server timeserver.example.org
server ntp2a.example.net

driftfile /var/db/ntp.drift
```

Η επιλογή `server` προσδιορίζει ποιοι εξυπηρετητές θα χρησιμοποιηθούν, παραθέτοντας έναν σε κάθε γραμμή. Αν ένας εξυπηρετητής φέρει το πρόθεμα `prefer`, όπως συμβαίνει με τον `ntplocal.example.com`, τότε αυτός ο εξυπηρετητής είναι ο προτιμώμενος. Θα απορριφθεί η απάντηση από τον προτιμώμενο εξυπηρετητή σε περίπτωση που διαφέρει σημαντικά από όλους τους άλλους εξυπηρετητές, Σε περίπτωση που δεν υπάρχει μεγάλη απόκλιση θα χρησιμοποιηθεί δίχως να ληφθούν υπόψιν οι άλλες απαντήσεις. Το πρόθεμα `prefer` συνήθως χρησιμοποιείται με εξυπηρετητές NTP ακριβείας, όπως αυτοί που φέρουν ειδικούς μηχανισμούς παρακολούθησης χρονισμού.

Η επιλογή `driftfile` προσδιορίζει ποιό αρχείο χρησιμοποιείται για να διατηρεί τη συχνότητα διόρθωσης του clock του συστήματος. Το πρόγραμμα ntpd(8) χρησιμοποιεί αυτόματα αυτή τη τιμή

για να αντισταθμίζει τις φυσικές αποκλίσεις του clock, επιτρέποντας του να διατηρεί μια λογική ρύθμιση, ακόμη κι αν του απαγορευτεί για κάποιο χρονικό διάστημα η πρόσβαση προς όλες τις εξωτερικές πηγές συγχρονισμού.

Η επιλογή `driftfile` προσδιορίζει ποιό αρχείο χρησιμοποιείται για να αποθηκεύει πληροφορίες σχετικά με τις προηγούμενες απαντήσεις από τους εξυπηρετητές NTP. Αυτό το αρχείο περιέχει εσωτερικές πληροφορίες του NTP. Δεν θα έπρεπε να τροποποιείτε από καμμία άλλη διεργασία.

54.10.3.3. Έλεγχος Πρόσβασης στον Εξυπηρετητή Σας

Προεπιλεγμένα, ο εξυπηρετητής σας NTP θα είναι προσβάσιμος από όλους τους κόμβους στο διαδίκτυο. Η επιλογή `restrict` στο /etc/ntp.conf σας επιτρέπει να ελέγχετε ποια μηχανήματα θα μπορούν να έχουν πρόσβαση στον εξυπηρετή σας.

Αν επιθυμείτε να απορρίψετε την πρόσβαση προς τον εξυπηρετητή σας NTP για όλα τα μηχανήματα, προσθέστε την ακόλουθη γραμμή στο /etc/ntp.conf:

```
restrict default ignore
```

Αν θέλετε μόνο να επιτρέψετε τον συγχρονισμό του εξυπηρετητή σας με μηχανήματα εντός του δικτύου σας, αλλά δίχως δυνατότητα ρύθμισης του εξυπηρετητή ή να γίνουν ομοιόβαθμα με άδεια συγχρονισμού, τότε αντιθέτως προσθέστε:

```
restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap
```

όπου `192.168.1.0` είναι η διεύθυνση IP του δικτύου και `255.255.255.0` είναι η μάσκα του δικτύου σας.

Το /etc/ntp.conf μπορεί να περιέχει πολλαπλές επιλογές `restrict`. Για περισσότερες πληροφορίες, δείτε την υποενότητα `Υποστήριξη Ελέγχου Πρόσβασης (Access Control Support)`, υποενότητα του ntp.conf(5).

54.10.4. Εκτέλεση του NTP Εξυπηρετητή Σας

Για να βεβαιωθείτε πως ο εξυπηρετητής NTP θα ξεκινάει κατά την διάρκεια εκκίνησης του συστήματος, προσθέστε τη γραμμή `ntpd_enable="YES"` στο /etc/rc.conf. Για να ξεκινήσετε τον εξυπηρετητή δίχως να επανεκκινήσετε το μηχάνημα σας, τρέξτε ntpd(8) προσδιορίζοντας κάθε επιπρόσθετη παράμετρο από τα `ntpd_flags` στο /etc/rc.conf. Για παράδειγμα:

```
# ntpd -p /var/run/ntpd.pid
```

54.10.5. Χρήση του ntpd με Προσωρινή Σύνδεση στο Ίντερνετ

Το πρόγραμμα ntpd(8) δεν χρειάζεται μια μόνιμη σύνδεση στο Ίντερνετ για να δουλέψει σωστά. Αν έχετε μια προσωρινή σύνδεση που είναι ρυθμισμένη να κάνει κλήσεις μέσω τηλεφώνου (dial out on demand), είναι καλό να μην είναι η κίνηση δεδομένων του NTP το αίτιο της κλήσης ή αυτή που θα κρατάει ενεργή την σύνδεση. Αν χρησιμοποιείτε PPP χρήστη, μπορείτε να χρησιμοποιήσετε `φίλτρα`

στους κώδικες παραπομπής του /etc/ppp/ppp.conf, όπως για παράδειγμα:

```
set filter dial 0 deny udp src eq 123
# Prevent NTP traffic from initiating dial out
set filter dial 1 permit 0 0
set filter alive 0 deny udp src eq 123
# Prevent incoming NTP traffic from keeping the connection open
set filter alive 1 deny udp dst eq 123
# Prevent outgoing NTP traffic from keeping the connection open
set filter alive 2 permit 0/0 0/0
```

Για περισσότερες λεπτομέρειες δείτε το `PACKET FILTERING` στην ενότητα ppp(8) και τα παραδείγματα στο /usr/shared/examples/ppp/.

Σημείωση: Μερικοί ISP μπλοκάρουν την χρήση θύρας με χαμηλό αριθμό, εμποδίζοντας στο NTP να δουλεύει αφού οι απαντήσεις δεν φτάνουν ποτέ στο μηχάνημα σας.

54.10.6. Περαιτέρω Πληροφορίες

Η τεκμηρίωση για τους εξυπηρετητές NTP διατίθεται και σε φόρμα HTML στο /usr/shared/doc/ntp/.

Chapter 55. Firewalls

55.1. Σύνοψη

Το firewall (τείχος προστασίας) καθιστά δυνατό το φιλτράρισμα της εισερχόμενης και εξερχόμενης κίνησης που διέρχεται από το σύστημα σας. Ένα firewall μπορεί να χρησιμοποιεί ένα ή περισσότερα σετ "κανόνων" για να επιθεωρεί τα πακέτα κατά την είσοδο ή έξοδο τους από μια δικτυακή σύνδεση, και να τα επιτρέπει ή να τα απορρίπτει. Οι κανόνες του firewall μπορούν να ελέγχουν ένα ή περισσότερα χαρακτηριστικά των πακέτων, συμπεριλαμβανομένων μεταξύ άλλων και του τύπου του πρωτοκόλλου, καθώς και την διεύθυνση ή/και θύρα (port) της αφετηρίας ή του προορισμού.

Τα firewalls μπορούν να ενισχύσουν σημαντικά την ασφάλεια ενός κόμβου ή ενός δικτύου. Μπορούν να χρησιμοποιηθούν για μία ή περισσότερες από τις ακόλουθες λειτουργίες:

- Να προστατεύουν και να απομονώνουν τις εφαρμογές, τις υπηρεσίες και τα μηχανήματα του εσωτερικού σας δικτύου από ανεπιθύμητη κίνηση που προέρχεται από το Internet.
- Να περιορίζουν ή να αποκλείουν την πρόσβαση μηχανημάτων του εσωτερικού δικτύου σε υπηρεσίες του Internet.
- Να υποστηρίζουν μετάφραση δικτυακών διευθύνσεων (NAT), η οποία επιτρέπει στο εσωτερικό σας δίκτυο να χρησιμοποιεί ιδιωτικές IP διευθύνσεις και να μοιράζεται μία μοναδική σύνδεση με το Internet (είτε μέσω μίας μοναδικής δημόσιας IP διεύθυνσης, είτε μέσω ενός πλήθους δημοσίων διευθύνσεων που ανατίθενται αυτόματα).

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Πως να δημιουργήσετε σωστούς κανόνες φιλτραρίσματος πακέτων.
- Τους διάφορους τύπους firewall που υπάρχουν στο FreeBSD και τις διαφορές τους.
- Πως να ρυθμίσετε και να χρησιμοποιήσετε το PF firewall του OpenBSD.
- Πως να ρυθμίσετε και να χρησιμοποιήσετε το IPFILTER.
- Πως να ρυθμίσετε και να χρησιμοποιήσετε το IPFW.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε βασικές αρχές του FreeBSD και του Internet.

55.2. Βασικές Έννοιες των Firewalls

Υπάρχουν δύο βασικοί τρόποι για τη δημιουργία κανόνων σε ένα firewall: ο "inclusive" και ο "exclusive". Ένα exclusive firewall επιτρέπει τη διέλευση όλης της κίνησης, εκτός από αυτή που ταιριάζει με τους κανόνες του. Ένα inclusive firewall κάνει το ανάποδο. Επιτρέπει μόνο τη διέλευση της κίνησης που ταιριάζει με τους κανόνες του, και αποκλείει οτιδήποτε άλλο.

Τα inclusive firewalls προσφέρουν πολύ καλύτερο έλεγχο της εξερχόμενης κίνησης και για το λόγο αυτό είναι καλύτερα για συστήματα που προσφέρουν υπηρεσίες στο δημόσιο Internet. Ελέγχουν επίσης και τα πακέτα που προέρχονται από το δημόσιο Internet με προορισμό το ιδιωτικό σας δίκτυο. Από προεπιλογή, όλη η κίνηση που δεν ταιριάζει με τους κανόνες απορρίπτεται και

καταγράφεται. Τα inclusive firewalls είναι γενικά ασφαλέστερα από τα exclusive, καθώς μειώνουν σημαντικά την πιθανότητα διέλευσης ανεπιθύμητης κίνησης μέσα από αυτά.

Εκτός και αν αναφέρεται διαφορετικά, όλα τα παραδείγματα ρυθμίσεων και κανόνων που φαίνονται σε αυτό το κεφάλαιο, δημιουργούν inclusive firewalls.

Η ασφάλεια μπορεί να γίνει ακόμα ισχυρότερη με τη χρήση ενός "stateful firewall". Αυτός ο τύπος firewall αποθηκεύει την κατάσταση των συνδέσεων που μεταφέρουν δεδομένα μέσα από αυτό, και επιτρέπει μόνο την κίνηση που είτε ταιριάζει με μια από τις υπάρχουσες συνδέσεις, ή που ξεκινά μια νέα σύνδεση. Το μειονέκτημα ενός stateful firewall είναι ότι μπορεί να είναι ευάλωτο σε επιθέσεις Denial of Service (Άρνησης Υπηρεσίας, DoS) αν δεχθεί ταυτόχρονα πολλές αιτήσεις για άνοιγμα νέων συνδέσεων σε μικρό χρονικό διάστημα. Με τα περισσότερα firewalls, είναι δυνατόν να γίνει συνδυασμός και των δύο συμπεριφορών (τόσο stateful όσο και μη-stateful) ώστε να δημιουργηθεί το βέλτιστο firewall για την συγκεκριμένη χρήση.

55.3. Προγράμματα Firewall

Το FreeBSD έχει τρία διαφορετικά προγράμματα firewall ενσωματωμένα στο βασικό σύστημα. Είναι τα: *IPFILTER* (γνωστό επίσης και ως IPF), το *IPFIREWALL* (γνωστό επίσης και ως IPFW), και το *PacketFilter* του *OpenBSD* (γνωστό επίσης και ως PF). Το FreeBSD ενσωματώνει επίσης δύο προγράμματα για διαμόρφωση κυκλοφορίας (traffic shaping, έλεγχος του διαθέσιμου εύρους ζώνης): το altq(4) και το dummynet(4). Το Dummynet είναι κατά παράδοση στενά συνδεμένο με το IPFW, και το ALTQ με το PF. Η διαμόρφωση κυκλοφορίας για το IPFILTER μπορεί τη δεδομένη στιγμή να γίνει με το IPFILTER για το NAT και το φιλτράρισμα και με το IPFW σε συνδυασμό με το dummynet(4) *ή* χρησιμοποιώντας το PF σε συνδυασμό με το ALTQ. Τόσο το IPFW όσο και το PF χρησιμοποιούν κανόνες για να ελέγξουν την κίνηση των πακέτων από και προς το σύστημά σας, αν και διαθέτουν διαφορετικούς τρόπους για να το επιτύχουν, και οι κανόνες τους χρησιμοποιούν διαφορετική σύνταξη.

Ο λόγος για τον οποίο το FreeBSD διαθέτει πολλαπλά firewall, είναι ότι διαφορετικοί άνθρωποι έχουν διαφορετικές ανάγκες και προτιμήσεις. Δεν υπάρχει ένα και μοναδικό firewall που να είναι το καλύτερο.

Ο συγγραφέας προτιμά το IPFILTER, καθώς οι κανόνες τύπου stateful που διαθέτει είναι λιγότερο πολύπλοκοι όταν χρησιμοποιούνται σε ένα περιβάλλον NAT, ενώ διαθέτει και ενσωματωμένο ftp proxy το οποίο τους απλοποιεί ακόμα περισσότερο, επιτρέποντας ασφαλή σύνδεση σε εξωτερικούς εξυπηρετητές FTP.

Καθώς όλα τα firewall βασίζονται στην επιθεώρηση τιμών ελέγχου των πακέτων, ο διαχειριστής που πρόκειται να δημιουργήσει τους κανόνες πρέπει να κατανοεί τον τρόπο λειτουργίας του TCP/IP, το ρόλο των διαφόρων τιμών στα πεδία ελέγχου των πακέτων και πως χρησιμοποιούνται στην ανταλλαγή πληροφοριών σε μια συνηθισμένη συνεδρία. Για περισσότερες λεπτομέρειες, διαβάστε το http://www.ipprimer.com/overview.cfm.

55.4. Το Packet Filter (PF) και το ALTQ του OpenBSD

Τον Ιούλιο του 2003, η εφαρμογή firewall του OpenBSD (γνωστή ως PF) μεταφέρθηκε στο FreeBSD και έγινε διαθέσιμη στην Συλλογή των Ports. Το FreeBSD 5.3 που κυκλοφόρησε το 2004, ήταν η

πρώτη επίσημη έκδοση η οποία περιείχε το PF ως τμήμα του βασικού πλέον συστήματος. Το PF είναι ένα ολοκληρωμένο firewall, με πλήθος χαρακτηριστικών, το οποίο επίσης διαθέτει προαιρετικά υποστήριξη για το ALTQ (Alternate Queuing). Το ALTQ προσφέρει υπηρεσίες Διασφάλισης Ποιότητας (Quality of Service, QoS).

Το OpenBSD Project κάνει εξαιρετική δουλειά στη συντήρηση του PF FAQ. Για το λόγο αυτό, η παρούσα ενότητα του Εγχειριδίου εστιάζει κυρίως στις ιδιαιτερότητες του PF όσο αφορά το FreeBSD, ενώ παρέχει και μερικές γενικές πληροφορίες σχετικά με τη χρήση του. Για πιο λεπτομερείς πληροφορίες σχετικά με τη χρήση του PF, παρακαλούμε διαβάστε το PF FAQ.

Περισσότερες πληροφορίες σχετικά με το PF στο FreeBSD μπορείτε να βρείτε στο http://pf4freebsd.love2party.net/.

55.4.1. Χρησιμοποιώντας τα Αρθρώματα Πυρήνα για το PF

Για να φορτώσετε το άρθρωμα πυρήνα για το PF, προσθέστε την παρακάτω γραμμή στο στο /etc/rc.conf:

```
pf_enable="YES"
```

Εκτελέστε έπειτα το script εκκίνησης για να φορτώσετε το άρθρωμα:

```
# /etc/rc.d/pf start
```

Σημειώστε ότι το άρθρωμα PF δεν πρόκειται να φορτωθεί αν δεν βρει το καθορισμένο αρχείο κανόνων. Το προεπιλεγμένο αρχείο είναι το /etc/pf.conf. Αν το αρχείο κανόνων βρίσκεται σε κάποια άλλη τοποθεσία, μπορείτε να την καθορίσετε προσθέτοντας μια γραμμή όπως την παρακάτω στο /etc/rc.conf:

```
pf_rules="/path/to/pf.conf"
```

Μπορείτε να βρείτε ένα παράδειγμα του αρχείου pf.conf στον κατάλογο /usr/shared/examples/pf

Το άρθρωμα PF μπορεί επίσης να φορτωθεί χειροκίνητα από την γραμμή εντολών:

```
# kldload pf.ko
```

Η υποστήριξης καταγραφής του PF παρέχεται από το άρθρωμα `pflog.ko` και μπορείτε να την φορτώσετε προσθέτοντας την παρακάτω γραμμή στο /etc/rc.conf:

```
pflog_enable="YES"
```

Εκτελέστε έπειτα το script εκκίνησης για να φορτώσετε το άρθρωμα:

```
# /etc/rc.d/pflog start
```

Αν χρειάζεστε κάποιο από τα προχωρημένα χαρακτηριστικά του PF, θα πρέπει να μεταγλωττίσετε την υποστήριξη για το PF απευθείας μέσα στον πυρήνα.

55.4.2. Επιλογές του PF για τον Πυρήνα

Αν και δεν είναι απαραίτητο να μεταγλωττίσετε την υποστήριξη PF μέσα στον πυρήνα του FreeBSD, ίσως να θέλετε να χρησιμοποιήσετε ένα από τα προχωρημένα χαρακτηριστικά του PF το οποίο δεν περιλαμβάνεται στο άρθρωμα του πυρήνα: το pfsync(4). Πρόκειται για μια ψευδο-συσκευή η οποία αποκαλύπτει συγκεκριμένες αλλαγές στον πίνακα καταστάσεων που χρησιμοποιείται από το PF. Μπορεί να συνδυαστεί με το carp(4) για να δημιουργηθούν με το PF firewalls με δυνατότητα αυτόματης αλλαγής σε περίπτωση αποτυχίας (failover). Περισσότερες πληροφορίες σχετικά με το CARP μπορείτε να βρείτε στο Common Access Redundancy Protocol (CARP) του Εγχειριδίου.

Μπορείτε να δείτε όλες τις επιλογές πυρήνα για το PF στο αρχείο /usr/src/sys/conf/NOTES. Οι επιλογές φαίνονται επίσης παρακάτω:

```
device pf
device pflog
device pfsync
```

Η επιλογή `device pf` ενεργοποιεί την υποστήριξη για το firewall "Packet Filter" (pf(4)).

Η επιλογή `device pflog` ενεργοποιεί την προαιρετική ψευδο-δικτυακή συσκευή pflog(4) που μπορεί να χρησιμοποιηθεί για την καταγραφή της κίνησης σε ένα bpf(4) descriptor. Ο δαίμονας pflogd(8) μπορεί να αποθηκεύσει την καταγραφή αυτή στο σκληρό δίσκο.

Η επιλογή `device pfsync` ενεργοποιεί την προαιρετική ψευδό-δικτυακή συσκευή pfsync(4) η οποία χρησιμοποιείται για να ανιχνεύει "αλλαγές κατάστασης".

55.4.3. Επιλογές στο rc.conf

Το PF και το pflog(4) μπορούν να ρυθμιστούν κατά την εκκίνηση με τις παρακάτω καταχωρίσεις στο rc.conf(5):

```
pf_enable="YES"                 # Enable PF (load module if required)
pf_rules="/etc/pf.conf"         # rules definition file for pf
pf_flags=""                     # additional flags for pfctl startup
pflog_enable="YES"              # start pflogd(8)
pflog_logfile="/var/log/pflog"  # where pflogd should store the logfile
pflog_flags=""                  # additional flags for pflogd startup
```

Αν πίσω από αυτό το firewall υπάρχει κάποιο τοπικό δίκτυο (LAN) προς το οποίο επιθυμείτε να προωθήσετε πακέτα, ή αν θέλετε να χρησιμοποιήσετε NAT, θα χρειαστείτε επίσης και την παρακάτω επιλογή:

```
gateway_enable="YES"            # Enable as LAN gateway
```

55.4.4. Δημιουργία Κανόνων Φιλτραρίσματος

Το PF διαβάζει τις ρυθμίσεις του από το pf.conf(5) (η προεπιλεγμένη τοποθεσία είναι στο /etc/pf.conf) και τροποποιεί, απορρίπτει ή αποδέχεται πακέτα σύμφωνα με τους κανόνες και τους ορισμούς που περιέχονται σε αυτό. Η εγκατάσταση του FreeBSD περιλαμβάνει αρκετά υποδείγματα αρχείων ρύθμισης, στην τοποθεσία /usr/shared/examples/pf/. Παρακαλούμε να διαβάσετε το PF FAQ για πλήρη ανάλυση των κανόνων του PF.

Καθώς διαβάζετε το PF FAQ, να έχετε υπόψη σας ότι διαφορετικές εκδόσεις του FreeBSD περιέχουν διαφορετικές εκδόσεις του PF. Τη δεδομένη στιγμή, το FreeBSD 8.*X* και οι προηγούμενες εκδόσεις χρησιμοποιούν την ίδια έκδοση του PF που χρησιμοποιεί και το OpenBSD 4.1. Το FreeBSD 9.*X* και νεώτερες εκδόσεις χρησιμοποιούν την ίδια έκδοση του PF με το OpenBSD 4.5.

Η ηλεκτρονική λίστα του FreeBSD για το packet filter firewall είναι ένα καλό μέρος για να κάνετε ερωτήσεις σχετικές με τη ρύθμιση και τη λειτουργία του PF firewall. Μη ξεχάσετε να ελέγξετε τα αρχεία της λίστας πριν ξεκινήσετε τις ερωτήσεις!

55.4.5. Δουλεύοντας με το PF

Χρησιμοποιήστε το pfctl(8) για να ελέγξετε το PF. Παρακάτω θα βρείτε κάποιες χρήσιμες εντολές (βεβαιωθείτε ότι έχετε διαβάσει τη σελίδα manual του pfctl(8) για να δείτε όλες τις διαθέσιμες επιλογές):

Εντολή	Σκοπός
`pfctl -e`	Ενεργοποίηση του PF
`pfctl -d`	Απενεργοποίηση του PF
`pfctl -F all -f /etc/pf.conf`	Διαγραφή όλων των κανόνων (nat, filter, state, table, κ.λ.π.) και εκ νέου ανάγνωση από το αρχείο /etc/pf.conf
`pfctl -s [ rules | nat | state ]`	Εκτύπωση αναφοράς σχετικά με τους κανόνες του φίλτρου, του NAT, ή του πίνακα κατάστασης
`pfctl -vnf /etc/pf.conf`	Ελέγχει το /etc/pf.conf για λάθη, αλλά δεν φορτώνει τους κανόνες

55.4.6. Ενεργοποίηση του ALTQ

Το ALTQ διατίθεται μόνο αν μεταγλωττίσετε απευθείας την υποστήριξη του μέσα στον πυρήνα του FreeBSD. Το ALTQ δεν υποστηρίζεται από όλα τα προγράμματα οδήγησης καρτών δικτύου. Παρακαλούμε δείτε τη σελίδα manual του altq(4) για τη λίστα των οδηγών που υποστηρίζονται στην έκδοση του FreeBSD που διαθέτετε.

Οι παρακάτω επιλογές του πυρήνα ενεργοποιούν το ALTQ και παρέχουν επιπρόσθετες λειτουργίες:

```
options         ALTQ
options         ALTQ_CBQ        # Class Bases Queuing (CBQ)
options         ALTQ_RED        # Random Early Detection (RED)
options         ALTQ_RIO        # RED In/Out
options         ALTQ_HFSC       # Hierarchical Packet Scheduler (HFSC)
options         ALTQ_PRIQ       # Priority Queuing (PRIQ)
options         ALTQ_NOPCC      # Required for SMP build
```

Η γραμμή `options ALTQ` ενεργοποιεί το πλαίσιο λειτουργιών ALTQ.

Η γραμμή `options ALTQ_CBQ` ενεργοποιεί το *Class Based Queuing* (CBQ). Το CBQ σας επιτρέπει να χωρίσετε το εύρος ζώνης μιας σύνδεσης σε διαφορετικές κλάσεις ή ουρές, ώστε να δίνονται προτεραιότητες στην κίνηση ανάλογα με τους κανόνες του φίλτρου.

Η γραμμή `options ALTQ_RED` ενεργοποιεί το *Random Early Detection* (RED). Το RED χρησιμοποιείται για να αποφευχθεί η συμφόρηση του δικτύου. Για το σκοπό αυτό, το RED μετράει το μήκος της ουράς και το συγκρίνει με το μέγιστο και ελάχιστο όριο της. Αν η ουρά είναι πάνω από το μέγιστο, όλα τα νέα πακέτα θα απορρίπτονται. Σύμφωνα και με το όνομα του, το RED απορρίπτει πακέτα από διάφορες συνδέσεις με τυχαίο τρόπο.

Η γραμμή `options ALTQ_RIO` ενεργοποιεί το *Random Early Detection In and Out*.

Η γραμμή `options ALTQ_HFSC` ενεργοποιεί το *Hierarchical Fair Service Curve Packet Scheduler*. Για περισσότερες πληροφορίες σχετικά με το HFSC δείτε: http://www-2.cs.cmu.edu/~hzhang/HFSC/main.html.

Η γραμμή `options ALTQ_PRIQ` ενεργοποιεί το *Priority Queuing* (PRIQ). Το PRIQ πάντοτε περνάει πρώτα την κίνηση με τη μεγαλύτερη προτεραιότητα.

Η γραμμή `options ALTQ_NOPCC` ενεργοποιεί την υποστήριξη SMP για το ALTQ. Η επιλογή αυτή απαιτείται σε συστήματα SMP.

55.5. Το IPFILTER (IPF) Firewall

Ο συγγραφέας του IPFILTER είναι ο Darren Reed. Το IPFILTER δεν εξαρτάται από το λειτουργικό σύστημα: είναι μια εφαρμογή ανοικτού κώδικα που έχει μεταφερθεί στο FreeBSD, το NetBSD, το OpenBSD, το SunOS™, το HP/UX και το Solaris™. Το IPFILTER είναι υπό διαρκή και ενεργή ανάπτυξη και συντήρηση, και κυκλοφορούν τακτικά οι νέες εκδόσεις του.

Το IPFILTER είναι ένα firewall και μηχανισμός NAT που λειτουργεί στον πυρήνα και μπορεί να ελέγχεται και να παρακολουθείται από προγράμματα χρήστη. Οι κανόνες του firewall μπορούν να τίθενται σε ισχύ ή να διαγράφονται μέσω του βοηθητικού προγράμματος ipf(8). Οι κανόνες για το NAT μπορούν να τίθενται σε ισχύ ή να διαγράφονται μέσω του βοηθητικού προγράμματος ipnat(1). Το βοηθητικό πρόγραμμα ipfstat(8) μπορεί να εκτυπώσει στατιστικά εκτέλεσης για το τμήμα του IPFILTER που εκτελείται στον πυρήνα. Το πρόγραμμα ipmon(8) μπορεί να καταγράψει τις ενέργειες του IPFILTER στο αρχεία καταγραφής συμβάντων του συστήματος.

Το IPF γράφηκε αρχικά χρησιμοποιώντας μια λογική επεξεργασίας κανόνων του τύπου "ο τελευταίο

κανόνας που ταιριάζει, είναι και ο νικητής" και χρησιμοποιούσε μόνο κανόνες τύπου stateless. Με την πάροδο του χρόνου, το IPF βελτιώθηκε για να περιλαμβάνει την επιλογή "quick" και την επιλογή "keep state" για stateful κανόνες. Οι επιλογές αυτές εκσυγχρόνισαν δραματικά τη λογική επεξεργασίας των κανόνων. Η επίσημη τεκμηρίωση του IPF καλύπτει μόνο τις παλιές παραμέτρους ρύθμισης και επεξεργασίας των κανόνων. Οι σύγχρονες λειτουργίες καλύπτονται μόνο ως πρόσθετες επιλογές, και έτσι δεν τονίζονται αρκετά τα πλεονεκτήματα τους στη δημιουργία ενός πολύ καλύτερου και ασφαλέστερου firewall.

Οι οδηγίες που περιέχονται σε αυτή την ενότητα, βασίζονται στη χρήση κανόνων που περιέχουν την επιλογή "quick" καθώς και την stateful επιλογή "keep state". Αυτό είναι και το βασικό πλαίσιο λειτουργιών για την δημιουργία του σετ κανόνων ενός inclusive firewall.

Για λεπτομέρειες σχετικά με τον παλιότερο τρόπο επεξεργασίας των κανόνων, δείτε: http://www.obfuscation.org/ipf/ipf-howto.html#TOC_1 και http://coombs.anu.edu.au/~avalon/ip-filter.html.

Μπορείτε να δείτε το IPF FAQ στην τοποθεσία http://www.phildev.net/ipf/index.html.

Μπορείτε να βρείτε τις παλαιότερες δημοσιεύσεις τις λίστας ταχυδρομείου του IPFILTER στο http://marc.theaimsgroup.com/?l=ipfilter. Παρέχεται δυνατότητα αναζήτησης.

55.5.1. Ενεργοποιώντας το IPF

Το IPF περιλαμβάνεται στη βασική εγκατάσταση του FreeBSD ως άρθρωμα το οποίο μπορεί να φορτωθεί χωριστά. Το σύστημα θα φορτώσει δυναμικά το άρθρωμα του IPF αν υπάρχει η καταχώριση `ipfilter_enable="YES"` στο αρχείο /etc/rc.conf. Το άρθρωμα έχει δημιουργηθεί με ενεργοποιημένη την δυνατότητα καταγραφής και με την επιλογή `default pass all`. Για να αλλάξετε αυτή την προεπιλογή σε `block all`, μπορείτε απλώς να προσθέσετε τον κανόνα απόρριψης (block all) στο τέλος των κανόνων σας. Δεν χρειάζεται να μεταγλωττίσετε την επιλογή IPF στο πυρήνα του FreeBSD για το σκοπό αυτό.

55.5.2. Επιλογές για τον Πυρήνα

Δεν είναι υποχρεωτικό να μεταγλωττίσετε τις παρακάτω επιλογές στον πυρήνα του FreeBSD για να ενεργοποιήσετε το IPF. Η παρουσίαση τους εδώ είναι καθαρά ενημερωτική. Αν μεταγλωττίσετε το IPF απευθείας στον πυρήνα, δεν θα χρησιμοποιηθεί ποτέ το αντίστοιχο άρθρωμα.

Στο αρχείο /usr/src/sys/conf/NOTES θα βρείτε παραδείγματα καταχωρίσεων IPF για το αρχείο ρύθμισης του πυρήνα. Οι επιλογές αυτές φαίνονται επίσης παρακάτω:

```
options IPFILTER
options IPFILTER_LOG
options IPFILTER_DEFAULT_BLOCK
```

Η επιλογή `options IPFILTER` ενεργοποιεί την υποστήριξη για το "IPFILTER" firewall.

Η επιλογή `options IPFILTER_LOG` ενεργοποιεί την υποστήριξη καταγραφής του IPF, η οποία γράφει στην ψευδο-συσκευή καταγραφής πακέτων ipl για κάθε κανόνα που περιλαμβάνει την επιλογή `log`.

Η επιλογή `options IPFILTER_DEFAULT_BLOCK` αλλάζει την προεπιλεγμένη συμπεριφορά, ώστε κάθε πακέτο που δεν ταιριάζει με κάποιο κανόνα `pass` του firewall, να απορρίπτεται αυτόματα.

Οι παραπάνω επιλογές θα ενεργοποιηθούν μόνο αφού μεταγλωττίσετε και εγκαταστήσετε ένα προσαρμοσμένο πυρήνα που να τις περιλαμβάνει.

55.5.3. Διαθέσιμες Επιλογές για το rc.conf

Χρειάζεστε τις παρακάτω καταχωρίσεις στο /etc/rc.conf για να ενεργοποιήσετε το IPF κατά την εκκίνηση του υπολογιστή:

```
ipfilter_enable="YES"             # Start ipf firewall
ipfilter_rules="/etc/ipf.rules"   # loads rules definition text file
ipmon_enable="YES"                # Start IP monitor log
ipmon_flags="-Ds"                 # D = start as daemon
                                  # s = log to syslog
                                  # v = log tcp window, ack, seq
                                  # n = map IP & port to names
```

Αν πίσω από αυτό το firewall υπάρχει κάποιο LAN που χρησιμοποιεί δεσμευμένες ιδιωτικές διευθύνσεις, θα χρειαστεί να προσθέσετε τις παρακάτω καταχωρίσεις για να ενεργοποιήσετε τη λειτουργία NAT:

```
gateway_enable="YES"              # Enable as LAN gateway
ipnat_enable="YES"                # Start ipnat function
ipnat_rules="/etc/ipnat.rules"    # rules definition file for ipnat
```

55.5.4. IPF

Η εντολή ipf(8) χρησιμοποιείται για να φορτώσει το αρχείο των κανόνων. Φυσιολογικά, θα δημιουργήσετε ένα αρχείο με τους δικούς σας προσαρμοσμένους κανόνες και θα αντικαταστήσετε με αυτό εξ'ολοκλήρου τους ενσωματωμένους κανόνες του firewall:

```
# ipf -Fa -f /etc/ipf.rules
```

Η επιλογή `-Fa` αδειάζει τους κανόνες από τους εσωτερικούς πίνακες του firewall.

Η επιλογή `-f` καθορίζει το αρχείο των κανόνων που θα φορτωθεί.

Αυτό σας δίνει την δυνατότητα να αλλάξετε το αρχείο κανόνων σας, να εκτελέσετε την εντολή IPF που αναφέραμε παραπάνω, και να ανανεώσετε με αυτό τον τρόπο τους κανόνες στο firewall που εκτελείται ήδη με καινούργιους, χωρίς να χρειαστεί να επανεκκινήσετε το σύστημα σας. Η μέθοδος αυτή είναι πολύ βολική για να δοκιμάσετε νέους κανόνες, καθώς μπορεί να επαναληφθεί όσες φορές θέλετε.

Δείτε τη σελίδα manual του ipf(8) για λεπτομέρειες σχετικά με τις υπόλοιπες επιλογές που μπορείτε να χρησιμοποιήσετε με την εντολή αυτή.

Η εντολή ipf(8) αναμένει ένα απλό αρχείο κειμένου ως αρχείο κανόνων. Δεν θα δεχθεί αρχείο κανόνων γραμμένο ως script με συμβολικές αντικαταστάσεις.

Υπάρχει ωστόσο τρόπος να γράψετε κανόνες IPF που να χρησιμοποιούν την ισχύ των συμβολικών αντικαταστάσεων. Για περισσότερες πληροφορίες, δείτε το Δημιουργία Script Κανόνων με Συμβολική Υποκατάσταση.

55.5.5. IPFSTAT

Η προεπιλεγμένη συμπεριφορά του ipfstat(8) είναι να ανακτά και να απεικονίζει το σύνολο των στατιστικών που συγκεντρώθηκαν ως αποτέλεσμα της εφαρμογής των κανόνων του χρήστη στα πακέτα που εισέρχονται και εξέρχονται από το firewall, από τη στιγμή της τελευταίας του εκκίνησης ή από τον τελευταίο τους μηδενισμό μέσω της εντολής `ipf -Z`.

Δείτε τη σελίδα manual ipfstat(8) για λεπτομέρειες.

Η προεπιλεγμένη έξοδος της εντολής ipfstat(8) θα μοιάζει με την παρακάτω:

```
input packets: blocked 99286 passed 1255609 nomatch 14686 counted 0
 output packets: blocked 4200 passed 1284345 nomatch 14687 counted 0
 input packets logged: blocked 99286 passed 0
 output packets logged: blocked 0 passed 0
 packets logged: input 0 output 0
 log failures: input 3898 output 0
 fragment state(in): kept 0 lost 0
 fragment state(out): kept 0 lost 0
 packet state(in): kept 169364 lost 0
 packet state(out): kept 431395 lost 0
 ICMP replies: 0 TCP RSTs sent: 0
 Result cache hits(in): 1215208 (out): 1098963
 IN Pullups succeeded: 2 failed: 0
 OUT Pullups succeeded: 0 failed: 0
 Fastroute successes: 0 failures: 0
 TCP cksum fails(in): 0 (out): 0
 Packet log flags set: (0)
```

Όταν χρησιμοποιηθεί η επιλογή `-i` για τα εισερχόμενα ή η επιλογή `-o` για τα εξερχόμενα πακέτα, η εντολή θα ανακτήσει και θα απεικονίσει την αντίστοιχη λίστα κανόνων που είναι εγκατεστημένη και χρησιμοποιείται από τον πυρήνα τη δεδομένη στιγμή.

Η εντολή `ipfstat -in` δείχνει ένα αριθμημένο πίνακα κανόνων για εισερχόμενα πακέτα.

Η εντολή `ipfstat -on` δείχνει ένα αριθμημένο πίνακα κανόνων για εξερχόμενα πακέτα.

Η έξοδος θα μοιάζει με την παρακάτω:

```
@1 pass out on xl0 from any to any
@2 block out on dc0 from any to any
```

```
@3 pass out quick on dc0 proto tcp/udp from any to any keep state
```

Η εντολή `ipfstat -ih` δείχνει τον πίνακα κανόνων για τα εισερχόμενα πακέτα, τοποθετώντας μπροστά από τον κάθε κανόνα ένα αριθμό που δείχνει πόσες φορές έχει χρησιμοποιηθεί.

Η εντολή `ipfstat -oh` δείχνει τον πίνακα κανόνων για τα εξερχόμενα πακέτα, τοποθετώντας μπροστά από τον κάθε κανόνα ένα αριθμό που δείχνει πόσες φορές έχει χρησιμοποιηθεί.

Η έξοδος θα μοιάζει με την παρακάτω:

```
2451423 pass out on xl0 from any to any
354727 block out on dc0 from any to any
430918 pass out quick on dc0 proto tcp/udp from any to any keep state
```

Μια από τις πιο σημαντικές λειτουργίες της εντολής `ipfstat` είναι η επιλογή `-t` η οποία απεικονίζει τον πίνακα καταστάσεων, με τρόπο όμοιο με αυτό που χρησιμοποιεί η εντολή top(1) για να δείξει τον πίνακα διεργασιών που εκτελούνται στο FreeBSD. Όταν το firewall σας δέχεται επίθεση, η λειτουργία αυτή σας δίνει την δυνατότητα να αναγνωρίσετε και να εστιάσετε στα ίδια τα πακέτα που την αποτελούν. Οι προαιρετικές υπο-επιλογές σας δίνουν την δυνατότητα να επιλέξετε το IP αφετηρίας ή προορισμού, την θύρα, ή το πρωτόκολλο το οποίο θέλετε να παρακολουθήσετε σε πραγματικό χρόνο. Δείτε τη σελίδα manual του ipfstat(8) για περισσότερες λεπτομέρειες.

55.5.6. IPMON

Για να λειτουργήσει σωστά η εντολή `ipmon`, θα πρέπει να ενεργοποιηθεί η επιλογή `IPFILTER_LOG` στον πυρήνα. Η εντολή αυτή διαθέτει δύο διαφορετικούς τρόπους λειτουργίας. Ο προεπιλεγμένος κανονικός τρόπος λειτουργίας ενεργοποιείται όταν η εντολή χρησιμοποιείται χωρίς την επιλογή `-D`.

Η εντολή μπορεί να χρησιμοποιηθεί σε λειτουργία δαίμονα όταν επιθυμείτε να έχετε ένα συνεχόμενο αρχείο καταγραφής ώστε να μπορείτε να εξετάσετε τις προηγούμενες εγγραφές. Αυτός είναι και ο τρόπος με τον οποίο έχει ρυθμιστεί να συνεργάζεται το FreeBSD με το IPFILTER. Το FreeBSD έχει ενσωματωμένη δυνατότητα εναλλαγής αρχείων καταγραφής. Για αυτό το λόγο, είναι καλύτερο η καταγραφή να γίνεται μέσω του syslogd(8) παρά σε ένα συνηθισμένο αρχείο. Από προεπιλογή, η ρύθμιση `ipmon_flags` στο αρχείο rc.conf χρησιμοποιεί τις επιλογές `-Ds`:

```
ipmon_flags="-Ds" # D = start as daemon
                  # s = log to syslog
                  # v = log tcp window, ack, seq
                  # n = map IP & port to names
```

Τα πλεονεκτήματα της καταγραφής είναι προφανή. Παρέχει την δυνατότητα επισκόπησης πληροφοριών όπως τα πακέτα που απορρίφθηκαν, τις διευθύνσεις από τις οποίες λήφθηκαν, και τον προορισμό τους. Έχετε έτσι ένα σημαντικό πλεονέκτημα όταν προσπαθείτε να αναγνωρίσετε ένα εισβολέα.

Ακόμα και όταν ενεργοποιήσετε την δυνατότητα καταγραφής, το IPF δεν θα καταγράψει τίποτα αν δεν έχει γίνει η αντίστοιχη ρύθμιση στους κανόνες. Ο διαχειριστής του firewall αποφασίζει για

ποιους κανόνες του σετ θέλει να ενεργοποιήσει την καταγραφή, και προσθέτει σε αυτούς την λέξη log. Φυσιολογικά, η καταγραφή ενεργοποιείται μόνο σε κανόνες που απορρίπτουν πακέτα.

Είναι πολύ συνηθισμένο να περιλαμβάνεται ένας κανόνας στο τέλος του συνόλου, που να απορρίπτει από προεπιλογή όλα τα πακέτα που φτάνουν μέχρι εκεί (default deny). Με τον τρόπο αυτό μπορείτε να δείτε όλα τα πακέτα που δεν ταίριαξαν με κανένα κανόνα του σετ.

55.5.7. Καταγραφή του IPMON

Το syslogd χρησιμοποιεί τη δική του ειδική μέθοδο για το διαχωρισμό των δεδομένων καταγραφής. Διαθέτει ειδικές ομαδοποιήσεις που ονομάζονται "facility" και "level". Όταν το IPMON χρησιμοποιείται με την επιλογή `-Ds`, χρησιμοποιεί από προεπιλογή το `local0` ως όνομα "facility". Αν το επιθυμείτε, μπορείτε να χρησιμοποιήσετε τα παρακάτω επίπεδα για περαιτέρω διαχωρισμό των δεδομένων καταγραφής:

```
LOG_INFO - packets logged using the "log" keyword as the action rather than pass or
block.
LOG_NOTICE - packets logged which are also passed
LOG_WARNING - packets logged which are also blocked
LOG_ERR - packets which have been logged and which can be considered short
```

Για να ρυθμίσετε το IPFILTER να καταγράφει όλα τα δεδομένα στο /var/log/ipfilter.log, θα χρειαστεί να δημιουργήσετε από πριν το αρχείο. Αυτό μπορεί να γίνει με την παρακάτω εντολή:

```
# touch /var/log/ipfilter.log
```

Η λειτουργία του syslogd(8) μπορεί να ρυθμιστεί με καταχωρίσεις στο αρχείο /etc/syslog.conf. Το αρχείο syslog.conf προσφέρει σημαντική ευελιξία στον τρόπο με τον οποίο το syslog αντιμετωπίζει τα μηνύματα συστήματος που προέρχονται από εφαρμογές όπως το IPF.

Προσθέστε την παρακάτω καταχώριση στο αρχείο /etc/syslog.conf:

```
local0.* /var/log/ipfilter.log
```

Το `local0.*` σημαίνει ότι θα γίνεται καταγραφή όλων των μηνυμάτων αυτού του τύπου στην τοποθεσία που έχει οριστεί.

Για να ενεργοποιήσετε τις αλλαγές στο /etc/syslog.conf θα πρέπει να επανεκκινήσετε το μηχάνημα ή να αναγκάσετε το syslogd(8) να ξαναδιαβάσει το /etc/syslog.conf, εκτελώντας την εντολή `/etc/rc.d/syslogd reload`

Μην ξεχάσετε να τροποποιήσετε το /etc/newsyslog.conf ώστε να εναλλάσσει το αρχείο καταγραφής που δημιουργήσατε παραπάνω.

55.5.8. Η Μορφή των Μηνυμάτων Καταγραφής

Τα μηνύματα που παράγονται από την `ipmon` αποτελούνται από πεδία δεδομένων που χωρίζονται

από λευκό διάστημα. Τα πεδία που είναι κοινά σε όλα τα μηνύματα, είναι τα παρακάτω:

1. Η ημερομηνία παραλαβής του πακέτου
2. Η ώρα παραλαβής του πακέτου. Έχει την μορφή HH:MM:SS.F, η οποία υποδηλώνει ώρες, λεπτά, δευτερόλεπτα και κλάσματα δευτερολέπτου (τα οποία μπορεί να είναι πολλά δεκαδικά ψηφία).
3. Το όνομα της διεπαφής στην οποία έγινε η επεξεργασία του πακέτου π.χ. dc0.
4. Ο αριθμός ομάδας και ο αύξων αριθμός του κανόνα, π.χ. `@0:17`.

Μπορείτε να δείτε τα παρακάτω με την εντολή `ipfstat -in`:

1. Το είδος της ενέργειας: p αν το πακέτο πέρασε, b αν το πακέτο απορρίφθηκε, S για σύντομο πακέτο, n αν δεν ταίριαξε με κανένα κανόνα, L για κανόνα με καταγραφή. Η σειρά προτεραιότητας στην απεικόνιση των παραπάνω, είναι S, p, b, n, L. Το κεφαλαίο P ή το B σημαίνουν ότι η καταγραφή του πακέτου έγινε λόγω κάποιας γενικής ρύθμισης καταγραφής και όχι εξαιτίας κάποιου κανόνα.
2. Οι διευθύνσεις. Πρόκειται στην πραγματικότητα για τρία πεδία: τη διεύθυνση και τη θύρα αφετηρίας (χωρίζονται με κόμμα), το σύμβολο → και την διεύθυνση και θύρα προορισμού, π.χ. `209.53.17.22,80 → 198.73.220.17,1722`.
3. Το `PR` ακολουθούμενο από το όνομα ή τον αριθμό του πρωτοκόλλου, π.χ. `PR tcp`.
4. Το `len` ακολουθούμενο από το μήκος της επικεφαλίδας και το συνολικό μήκος του πακέτου, π.χ. `len 20 40`.

Αν πρόκειται για πακέτο TCP, θα υπάρχει ένα επιπλέον πεδίο το οποίο θα ξεκινάει με μια παύλα και θα ακολουθείται από γράμματα τα οποία αντιστοιχούν στις επιλογές (flags) που έχουν τεθεί. Δείτε τη σελίδα manual ipf(5) για τη λίστα των γραμμάτων και των αντίστοιχων flags.

Αν πρόκειται για πακέτο ICMP, θα υπάρχουν δύο πεδία στο τέλος, το πρώτο θα είναι πάντα "ICMP" και το επόμενο θα είναι ο τύπος του μηνύματος και του υπό-μηνύματος ICMP, χωρισμένα με μια κάθετο, π.χ. ICMP 3/3 για ένα μήνυμα μη προσβάσιμης θύρας (port unreachable).

55.5.9. Δημιουργία Script Κανόνων με Συμβολική Υποκατάσταση

Ορισμένοι έμπειροι χρήστες του IPF δημιουργούν ένα αρχείο κανόνων το οποίο μπορεί να εκτελεστεί ως script με δυνατότητα συμβολικής υποκατάστασης. Το βασικό όφελος του παραπάνω, είναι ότι χρειάζεται να αλλάξετε μόνο την τιμή που σχετίζεται με το συμβολικό όνομα και όταν το script εκτελεστεί, η τιμή θα υποκατασταθεί σε όλους τους κανόνες που περιέχουν το όνομα αυτό. Καθώς πρόκειται για script, μπορείτε να χρησιμοποιήσετε συμβολική υποκατάσταση για να κωδικοποιήσετε συχνά χρησιμοποιούμενες τιμές και να τις υποκαθιστάτε σε πολλαπλούς κανόνες. Αυτό φαίνεται και στο παράδειγμα που ακολουθεί.

Η σύνταξη του script που χρησιμοποιείται εδώ, είναι συμβατή με τα κελύφη sh(1), csh(1), και tcsh(1).

Τα πεδία στα οποία γίνεται συμβολική υποκατάσταση προσημειώνονται με το σήμα του δολαρίου: `$`.

Τα συμβολικά πεδία δεν έχουν την προσημείωση με το $.

Η τιμή που θα χρησιμοποιηθεί στο συμβολικό πεδίο, θα πρέπει να εσωκλείεται σε διπλά εισαγωγικά (").

Ξεκινήστε το αρχείο των κανόνων σας με κάτι αντίστοιχο με το παρακάτω:

```
############## Start of IPF rules script ##########################

oif="dc0"            # name of the outbound interface
odns="192.0.2.11"    # ISP's DNS server IP address
myip="192.0.2.7"     # my static IP address from ISP
ks="keep state"
fks="flags S keep state"

# You can choose between building /etc/ipf.rules file
# from this script or running this script "as is".
#
# Uncomment only one line and comment out another.
#
# 1) This can be used for building /etc/ipf.rules:
#cat > /etc/ipf.rules << EOF
#
# 2) This can be used to run script "as is":
/sbin/ipf -Fa -f - << EOF

# Allow out access to my ISP's Domain name server.
pass out quick on $oif proto tcp from any to $odns port = 53 $fks
pass out quick on $oif proto udp from any to $odns port = 53 $ks

# Allow out non-secure standard www function
pass out quick on $oif proto tcp from $myip to any port = 80 $fks

# Allow out secure www function https over TLS SSL
pass out quick on $oif proto tcp from $myip to any port = 443 $fks
EOF
################## End of IPF rules script ########################
```

Αυτό είναι όλο. Στο παραπάνω παράδειγμα δεν είναι σημαντικοί οι κανόνες, αλλά ο τρόπος με τον οποίο λειτουργούν και παίρνουν τιμές τα πεδία υποκατάστασης. Αν το παραπάνω παράδειγμα βρίσκονταν σε ένα αρχείο με το όνομα /etc/ipf.rules.script, θα μπορούσατε να επαναφορτώσετε αυτούς τους κανόνες με την παρακάτω εντολή:

```
# sh /etc/ipf.rules.script
```

Υπάρχει ένα πρόβλημα όταν χρησιμοποιούνται αρχεία κανόνων με ενσωματωμένους συμβολισμούς: Το IPF δεν καταλαβαίνει τη συμβολική υποκατάσταση, και δεν μπορεί να διαβάσει αυτά τα scripts άμεσα.

Ένα τέτοιο script μπορεί να χρησιμοποιηθεί με ένα από τους δύο παρακάτω τρόπους:

- Αφαιρέστε το σχόλιο από τη γραμμή που ξεκινάει με `cat`, και μετατρέψτε σε σχόλιο τη γραμμή που ξεκινάει με `/sbin/ipf`. Τοποθετήστε το `ipfilter_enable="YES"` στο αρχείο /etc/rc.conf όπως

συνήθως, και εκτελέστε το script μια φορά μετά από κάθε αλλαγή για να δημιουργήσετε ή να ενημερώσετε το /etc/ipf.rules.

- Απενεργοποιήστε το IPFILTER στα scripts εκκίνησης του συστήματος, προσθέτοντας την καταχώριση `ipfilter_enable="NO"` (πρόκειται για την προεπιλεγμένη τιμή) στο αρχείο /etc/rc.conf.

  Προσθέστε ένα script όπως το παρακάτω στον κατάλογο εκκίνησης /usr/local/etc/rc.d/. Το script θα πρέπει να έχει ένα προφανές όνομα, όπως ipf.loadrules.sh. Η επέκταση .sh είναι υποχρεωτική.

  ```
  #!/bin/sh
  sh /etc/ipf.rules.script
  ```

  Οι άδειες σε αυτό το αρχείο, θα πρέπει να επιτρέπουν ανάγνωση, εγγραφή και εκτέλεση για τον χρήστη `root`.

  ```
  # chmod 700 /usr/local/etc/rc.d/ipf.loadrules.sh
  ```

Οι κανόνες του IPF θα φορτώνονται πλέον κατά την εκκίνηση του συστήματος σας.

55.5.10. Το Σύνολο Κανόνων του IPF

Ως "σύνολο κανόνων" στο IPF, ορίζουμε μια ομάδα κανόνων που έχουν γραφεί για να επιτρέπουν ή να απορρίπτουν πακέτα ανάλογα με τις τιμές που περιέχονται σε αυτά. Η διπλής κατεύθυνσης ανταλλαγή πακέτων μεταξύ υπολογιστών αποτελεί μια συνεδρία. Το σύνολο κανόνων του firewall επεξεργάζεται τόσο τα πακέτα που έρχονται από το Internet, όσο και τα πακέτα που παράγονται από το σύστημα ως απάντηση σε αυτά. Κάθε υπηρεσία TCP/IP (π.χ. telnet, www, mail, κ.λ.π.) καθορίζεται από το πρωτόκολλο και την προνομιακή (privileged) θύρα που χρησιμοποιεί για να δέχεται αιτήματα εξυπηρέτησης. Τα πακέτα που προορίζονται για μια συγκεκριμένη υπηρεσία, ξεκινούν από τη διεύθυνση αφετηρίας χρησιμοποιώντας μια μη-προνομιακή θύρα και καταλήγουν στη συγκεκριμένη θύρα υπηρεσίας στον προορισμό. Όλες οι παραπάνω παράμετροι (θύρες και διευθύνσεις) μπορούν να χρησιμοποιηθούν ως κριτήρια επιλογής για την δημιουργία κανόνων που επιτρέπουν ή εμποδίζουν την πρόσβαση σε υπηρεσίες.

Το IPF γράφτηκε αρχικά χρησιμοποιώντας μια λογική επεξεργασίας κανόνων του τύπου "ο τελευταίος κανόνας που ταιριάζει, είναι ο νικητής" και χρησιμοποιούσε μόνο κανόνες stateless. Με την πάροδο του χρόνου, το IPF ενισχύθηκε με την επιλογή "quick" και με δυνατότητα αποθήκευσης κατάστασης μέσω της επιλογής "keep state". Με τον τρόπο αυτό, εκσυγχρονίστηκε δραματικά η λογική επεξεργασίας των κανόνων.

Οι οδηγίες που περιέχονται σε αυτή την ενότητα βασίζονται στη χρήση κανόνων που περιέχουν την επιλογή "quick" και την επιλογή "keep state" για τη διατήρηση της κατάστασης. Αυτές είναι και οι βασικές λειτουργίες για την κωδικοποίηση του συνόλου κανόνων ενός inclusive firewall.

Όταν δουλεύετε με τους κανόνες του firewall, θα πρέπει να είστε *πολύ προσεκτικοί*. Αν βάλετε λανθασμένες ρυθμίσεις, μπορεί να *κλειδωθείτε έξω* από τον

> εξυπηρετητή σας. Για να είστε ασφαλείς, είναι προτιμότερο να κάνετε τις αρχικές σας ρυθμίσεις από την τοπική κονσόλα, παρά μέσω απομακρυσμένης σύνδεσης (π.χ. μέσω ssh).

55.5.11. Συντακτικό Κανόνων

Το συντακτικό των κανόνων που παρουσιάζουμε εδώ, έχει απλοποιηθεί ώστε να απεικονίζει τη σύγχρονη stateful υλοποίηση και τη λογική του τύπου "ο πρώτος κανόνας που ταιριάζει είναι και ο νικητής". Για την περιγραφή του παλιότερου τρόπου λειτουργίας, διαβάστε τη σελίδα manual του ipf(8).

Ο χαρακτήρας `#` χρησιμοποιείται για να επισημάνει την αρχή ενός σχολίου, και μπορεί να εμφανίζεται στο τέλος μιας γραμμής κανόνα ή στη δική του γραμμή. Οι κενές γραμμές αγνοούνται.

Οι κανόνες περιέχουν λέξεις-κλειδιά. Οι λέξεις αυτές θα πρέπει να κωδικοποιηθούν με συγκεκριμένη σειρά από τα αριστερά προς τα δεξιά της γραμμής. Οι λέξεις-κλειδιά φαίνονται παρακάτω με έντονα γράμματα. Μερικές λέξεις έχουν υπο-επιλογές οι οποίες μπορεί να είναι επίσης λέξεις-κλειδιά και να περιλαμβάνουν επίσης περισσότερες υπο-επιλογές. Κάθε μια από τις επικεφαλίδες στο παράδειγμα που φαίνεται παρακάτω έχει μια κεφαλίδα με έντονα γράμματα η οποία επεξηγεί το περιεχόμενο της.

`ACTION IN-OUT OPTIONS SELECTION STATEFUL PROTO SRC_ADDR,DST_ADDR OBJECT PORT_NUM TCP_FLAG STATEFUL`

`ACTION` = block | pass

`IN-OUT` = in | out

`OPTIONS` = log | quick | on interface-name

`SELECTION` = proto value | source/destination IP | port = number | flags flag-value

`PROTO` = tcp/udp | udp | tcp | icmp

`SRC_ADD,DST_ADDR` = all | from object to object

`OBJECT` = IP address | any

`PORT_NUM` = port number

`TCP_FLAG` = S

`STATEFUL` = keep state

55.5.11.1. ACTION

Η ενέργεια (action) δείχνει τι πρέπει να γίνει με το πακέτο αν ταιριάζει με τον κανόνα του φίλτρου. Κάθε κανόνας *πρέπει* να διαθέτει μια ενέργεια. Οι ενέργειες που αναγνωρίζονται, φαίνονται παρακάτω:

Το `block` δείχνει ότι το πακέτο θα πρέπει να απορριφθεί αν ταιριάζει με τις παραμέτρους επιλογής του κανόνα.

Το pass δείχνει ότι το πακέτο θα πρέπει να εξέλθει από το firewall, αν ταιριάζει με τις παραμέτρους επιλογής του κανόνα.

55.5.11.2. IN-OUT

Κάθε κανόνας του φίλτρου πρέπει υποχρεωτικά να διευκρινίζει με σαφήνεια αν αναφέρεται στην είσοδο ή την έξοδο πακέτων. Η επόμενη λέξη-κλειδί πρέπει να είναι in ή out και αν δεν υπάρχει, ο κανόνας θα αποτύχει κατά το συντακτικό έλεγχο.

Το in σημαίνει ότι ο κανόνας θα εφαρμοστεί σε ένα εισερχόμενο πακέτο το οποίο μόλις λήφθηκε στη διεπαφή που συνδέεται με το Διαδίκτυο.

Το out σημαίνει ότι ο κανόνας θα εφαρμοστεί σε ένα πακέτο που προορίζεται για έξοδο μέσω της διεπαφής που συνδέεται με το Διαδίκτυο.

55.5.11.3. OPTIONS

Οι παρακάτω επιλογές πρέπει να χρησιμοποιηθούν με τη σειρά που φαίνονται εδώ.

Το log δείχνει ότι η επικεφαλίδα του πακέτου θα γραφεί στο αρχείο καταγραφής του ipl (όπως περιγράφεται στην ενότητα LOGGING που ακολουθεί) αν οι παράμετροι της επιλογής ταιριάζουν με το πακέτο.

Το quick δείχνει ότι αν οι παράμετροι της επιλογής ταιριάζουν με το πακέτο, ο συγκεκριμένος κανόνας θα είναι και ο τελευταίος κανόνας που θα ελεγχθεί. Η επιλογή αυτή είναι υποχρεωτική για τη σύγχρονη λογική επεξεργασίας πακέτων.

Το on δείχνει το όνομα της διεπαφής που θα ενσωματωθεί στις παραμέτρους επιλογής. Τα ονόματα των διεπαφών φαίνονται όταν εκτελείται η εντολή ifconfig(8). Χρησιμοποιώντας την επιλογή αυτή, ο κανόνας θα ελεγχθεί μόνο αν το πακέτο διέρχεται μέσω της συγκεκριμένης διεπαφής και προς τη συγκεκριμένη κατεύθυνση (εισερχόμενα/εξερχόμενα). Η επιλογή αυτή είναι υποχρεωτική για την σύγχρονη λογική επεξεργασίας των κανόνων.

Όταν γίνεται καταγραφή ενός πακέτου, οι επικεφαλίδες γράφονται στην ψευδο-συσκευή καταγραφής πακέτων IPL. Μετά την εντολή log, μπορούν να χρησιμοποιηθούν οι παρακάτω παράμετροι (με τη σειρά που φαίνονται):

Το body δείχνει ότι θα γίνει καταγραφή των πρώτων 128 bytes των περιεχομένων του πακέτου, που βρίσκονται αμέσως μετά την επικεφαλίδα.

Η επιλογή first συνίσταται να χρησιμοποιηθεί αν η επιλογή log χρησιμοποιείται σε συνδυασμό με την keep state. Με τον τρόπο αυτό γίνεται καταγραφή μόνο του πρώτου πακέτου (με το οποίο ξεκίνησε η επικοινωνία), και όχι όλων των υπολοίπων τα οποία ταιριάζουν με την πληροφορία "keep state".

55.5.11.4. SELECTION

Οι λέξεις κλειδιά που περιγράφονται σε αυτή την ενότητα, χρησιμοποιούνται για να περιγράψουν ποιες ιδιότητες του πακέτου θα διερευνηθούν για να καθοριστεί αν ταιριάζει ή όχι με τους κανόνες. Μια λέξη-κλειδί ορίζει το κεντρικό θέμα και ακολουθείται από άλλες λέξεις που ορίζουν τις ακριβείς

επιλογές. Πρέπει πάντοτε να επιλέγεται μια από αυτές τις λέξεις. Παρέχονται οι παρακάτω ιδιότητες γενικής χρήσης οι οποίες πρέπει να χρησιμοποιηθούν με αυτή τη σειρά:

55.5.11.5. PROTO

Το `proto` είναι η βασική λέξη, και πρέπει να γράφεται μαζί με κάποια αντίστοιχη τιμή για περαιτέρω επιλογή. Η τιμή επιτρέπει το ταίριασμα με ένα συγκεκριμένο πρωτόκολλο. Είναι υποχρεωτικό να χρησιμοποιηθεί για να λειτουργεί η σύγχρονη λογική επεξεργασίας των κανόνων.

Τα ονόματα πρωτοκόλλων που αναγνωρίζονται και μπορούν να χρησιμοποιηθούν, είναι τα `tcp/udp | udp | tcp | icmp` ή οποιαδήποτε άλλα εμφανίζονται στο /etc/protocols. Μπορείτε να χρησιμοποιήσετε το ειδικό όνομα `tcp/udp` το οποίο ταιριάζει είτε με πακέτο TCP είτε με UDP. Η ειδική αυτή ονομασία προστέθηκε ώστε να αποφεύγονται διπλοί, αλλά κατά τα άλλα όμοιοι, κανόνες.

55.5.11.6. SRC_ADDR/DST_ADDR

Η λέξη `all` είναι ουσιαστικά συνώνυμη με την φράση "from any to any" χωρίς να υπάρχουν άλλες παράμετροι για το ταίριασμα.

Όταν χρησιμοποιείται το `from src to dst`, οι λέξεις `from` και `to` δηλώνουν διευθύνσεις IP που θα χρησιμοποιηθούν για το ταίριασμα. Οι κανόνες πρέπει να καθορίζουν τις παραμέτρους τόσο της αφετηρίας όσο και του προορισμού. Η λέξη `any` έχει την ειδική ιδιότητα να ταιριάζει με οποιαδήποτε διεύθυνση IP. Παραδείγματα χρήσης: `from any to any` ή `from 0.0.0.0/0 to any` ή `from any to 0.0.0.0/0` ή `from 0.0.0.0 to any` ή `from any to 0.0.0.0`.

Δεν υπάρχει τρόπος να περιγραφούν περιοχές IP διευθύνσεων που δεν μπορούν να εκφραστούν εύκολα με τη μορφή αριθμών χωρισμένων με τελείες / μάσκας υποδικτύου. Μπορείτε να χρησιμοποιήσετε το βοηθητικό πρόγραμμα net-mgmt/ipcalc για διευκόλυνση σας στους υπολογισμούς. Δείτε την δικτυακή τοποθεσία του προγράμματος για περισσότερες πληροφορίες: http://jodies.de/ipcalc.

55.5.11.7. PORT

Το ταίριασμα με κάποια συγκεκριμένη θύρα αφετηρίας ή/και προορισμού (αν υπάρχει) εφαρμόζεται μόνο σε πακέτα TCP και UDP. Κατά την δημιουργία συγκρίσεων με θύρες, μπορείτε είτε να χρησιμοποιήσετε τον αριθμό της θύρας, είτε το όνομα της αντίστοιχης υπηρεσίας από το αρχείο /etc/services. Όταν η θύρα εμφανίζεται ως τμήμα του αντικειμένου `from`, το ταίριασμα θα γίνει με την θύρα της αφετηρίας. Όταν εμφανίζεται ως τμήμα του αντικειμένου `to`, το ταίριασμα θα γίνει με τη θύρα προορισμού. Για να λειτουργεί η σύγχρονη λογική ταιριάσματος κανόνων, θα πρέπει οπωσδήποτε να υπάρχει η επιλογή θύρας στο αντικείμενο `to`. Παράδειγμα χρήσης: `from any to any port = 80`

Οι συγκρίσεις που αναφέρονται σε μια μόνο θύρα, μπορούν να γίνουν με πολλούς διαφορετικούς τρόπους, χρησιμοποιώντας διαφορετικούς τελεστές σύγκρισης. Είναι επίσης δυνατόν να καθοριστούν ολόκληρες περιοχές από θύρες.

port "=" | "!=" | "<" | ">" | "⇐" | ">=" | "eq" | "ne" | "lt" | "gt" | "le" | "ge".

Για να καθορίσετε περιοχές θυρών, χρησιμοποιήστε port "<>" | "><"

Μετά τις παραμέτρους για το ταίριασμα της αφετηρίας και του προορισμού, οι παρακάτω δύο παράμετροι είναι υποχρεωτικές για να λειτουργεί η σύγχρονη λογική επεξεργασίας των κανόνων.

55.5.11.8. TCP_FLAG

Τα flags είναι ενεργά μόνο στο φιλτράρισμα του πρωτοκόλλου TCP. Το κάθε γράμμα αντιπροσωπεύει ένα πιθανό flag το για το οποίο γίνεται ανίχνευση στην επικεφαλίδα του πακέτου TCP.

Η σύγχρονη λογική επεξεργασίας των κανόνων, χρησιμοποιεί την παράμετρο `flags S` για την αναγνώριση της έναρξης μια συνεδρίας tcp.

55.5.11.9. STATEFUL

Σε ένα κανόνα που επιτρέπει (pass) το πέρασμα των πακέτων, η επιλογή `keep state` δείχνει ότι θα πρέπει να ενεργοποιείται η λειτουργία stateful filtering όταν το πακέτο ταιριάζει με τα κριτήρια επιλογής.

Η επιλογή αυτή είναι υποχρεωτική για τη λειτουργία της σύγχρονης λογικής επεξεργασίας κανόνων.

55.5.12. Φιλτράρισμα με Διατήρηση της Κατάστασης (stateful)

Το stateful φιλτράρισμα, αντιμετωπίζει την κίνηση του δικτύου ως μιας διπλής κατεύθυνσης ανταλλαγή πακέτων τα οποία δημιουργούν μια συνεδρία. Όταν ενεργοποιηθεί, η διατήρηση της κατάστασης (keep-state) δημιουργεί δυναμικά εσωτερικούς κανόνες για κάθε πακέτο το οποίο ανταλλάσσεται κατά τη διάρκεια αυτής της συνεδρίας. Έχει επίσης τη δυνατότητα να διερευνήσει αν ακολουθούνται οι έγκυροι κανόνες ανταλλαγής μηνυμάτων μεταξύ του αποστολέα και του παραλήπτη. Οποιαδήποτε πακέτα δεν ταιριάζουν με το πρότυπο αυτής της επικοινωνίας, απορρίπτονται ως ψεύτικα.

Η διατήρηση της κατάστασης επιτρέπει επίσης να περάσουν τα πακέτα ICMP που σχετίζονται με μια συνεδρία TCP ή UDP. Έτσι, αν ληφθούν πακέτα ICMP τύπου 3 code 4 ως απάντηση κατά τη διάρκεια της επίσκεψης σας σε μια ιστοσελίδα, (η οποία επιτρέπεται από τον αντίστοιχο κανόνα εξερχομένων), θα τους επιτραπεί η είσοδος. Οποιοδήποτε πακέτο για το οποίο το IPF είναι σίγουρο ότι πρόκειται για τμήμα μιας ενεργής συνεδρίας, θα περάσει ακόμα και αν είναι διαφορετικό πρωτόκολλο.

Αυτό που συμβαίνει είναι το παρακάτω:

Τα πακέτα που προορίζονται να εξέλθουν μέσω της διεπαφής που συνδέεται στο Internet, ελέγχονται αρχικά σύμφωνα με το δυναμικό πίνακα καταστάσεων. Αν το πακέτο ταιριάζει με το επόμενο που αναμένεται σε μια ενεργή συνεδρία, εξέρχεται από το firewall και ταυτόχρονα ενημερώνεται η κατάσταση της συγκεκριμένης συνεδρίας στον παραπάνω δυναμικό πίνακα. Τα υπόλοιπα πακέτα (που δεν ταιριάζουν με κάποια συνεδρία σε εξέλιξη) ελέγχονται σύμφωνα με το σύνολο κανόνων για τα εξερχόμενα πακέτα.

Τα πακέτα που έρχονται από τη διεπαφή που είναι συνδεμένη με το Internet, ελέγχονται αρχικά μέσω του δυναμικού πίνακα καταστάσεων. Αν το πακέτο ταιριάζει με το επόμενο που αναμένεται σε

μια ενεργή συνεδρία, εξέρχεται από το firewall και ταυτόχρονα ενημερώνεται η κατάσταση της συγκεκριμένης συνεδρίας στον παραπάνω πίνακα. Τα υπόλοιπα πακέτα (που δεν ταιριάζουν με κάποια συνεδρία σε εξέλιξη) ελέγχονται σύμφωνα με το σύνολο κανόνων για τα εισερχόμενα πακέτα.

Όταν η επικοινωνία ολοκληρωθεί, διαγράφεται από τον δυναμικό πίνακα καταστάσεων.

Το stateful φιλτράρισμα επιτρέπει να εστιάσουμε την προσοχή μας στην αποδοχή ή απόρριψη των νέων συνδέσεων. Αν επιτραπεί μια νέα συνεδρία, όλα τα υπόλοιπα πακέτα της θα επιτρέπονται αυτόματα, ενώ τυχόν ψεύτικα πακέτα θα απορρίπτονται επίσης αυτόματα. Το stateful φιλτράρισμα διαθέτει μια σειρά από προχωρημένες ικανότητες διερεύνησης των πακέτων, με δυνατότητα να αμύνεται σε πολλές διαφορετικές μεθόδους που χρησιμοποιούν οι επιτιθέμενοι.

55.5.13. Παράδειγμα Συνόλου Κανόνων για ένα Inclusive Firewall

Το παρακάτω σύνολο κανόνων δίνεται ως παράδειγμα για να φτιάξετε ένα ιδιαίτερα ασφαλές inclusive firewall. Ένα inclusive firewall επιτρέπει το πέρασμα μόνο των υπηρεσιών που ταιριάζουν με τους κανόνες που έχει για αποδοχή πακέτων, και απορρίπτει όλα τα υπόλοιπα. Τα firewalls που προστατεύουν άλλα μηχανήματα (τα οποία καλούνται και "network firewalls") θα πρέπει να διαθέτουν τουλάχιστον δύο διεπαφές. Η μια διεπαφή συνδέεται με το τοπικό δίκτυο (LAN) το οποίο θεωρείται έμπιστο, και η άλλη με το δημόσιο Internet. Εναλλακτικά, ένα firewall μπορεί να προστατεύει μόνο το σύστημα στο οποίο εκτελείται-αυτό καλείται "host based firewall" και είναι κατάλληλο ιδιαίτερα για εξυπηρετητές που λειτουργούν σε μη έμπιστα δίκτυα.

Όλα τα συστήματα τύπου UNIX®, συμπεριλαμβανομένου και του FreeBSD, έχουν σχεδιαστεί να χρησιμοποιούν την διεπαφή lo0 και την IP διεύθυνση `127.0.0.1` για εσωτερική επικοινωνία μέσα στο ίδιο το λειτουργικό σύστημα. Το firewall πρέπει να περιέχει κανόνες που να επιτρέπουν την ελεύθερη και χωρίς περιορισμούς κίνηση των ειδικών αυτών εσωτερικών πακέτων.

Οι κανόνες που εξουσιοδοτούν την πρόσβαση προς το Internet, ορίζονται στην διεπαφή του δικτύου που συνδέεται σε αυτό. Οι κανόνες αυτοί ελέγχουν τόσο την εισερχόμενη όσο και την εξερχόμενη κίνηση στο Internet. Η διεπαφή αυτή μπορεί να είναι η tun0 που χρησιμοποιείται στο PPP χρήστη, ή ακόμα και η κάρτα δικτύου που συνδέεται σε ένα DSL router ή modem.

Σε περίπτωση που μια ή περισσότερες κάρτες δικτύου συνδέονται σε εσωτερικά ιδιωτικά δίκτυα πίσω από το firewall, θα πρέπει να υπάρχουν οι αντίστοιχοι κανόνες που να επιτρέπουν την ελεύθερη διακίνηση των πακέτων ανάμεσα στις διεπαφές αυτές ή/και στο Internet.

Οι κανόνες πρέπει να οργανώνονται σε τρεις κύριες ενότητες: αρχικά όλες οι διεπαφές στις οποίες επιτρέπεται η ελεύθερη διακίνηση δεδομένων, έπειτα η διεπαφή από την οποία εξέρχονται τα πακέτα προς το δημόσιο δίκτυο (Internet) και τέλος η διεπαφή από την οποία λαμβάνονται πακέτα από το Internet.

Σε κάθε μια από τις ενότητες των διεπαφών που συνδέονται στο Internet, πρέπει να τοποθετούνται πρώτοι οι κανόνες που ταιριάζουν συχνότερα με την αντίστοιχη κίνηση. Ο τελευταίος κανόνας της ενότητας θα πρέπει να απορρίπτει και να καταγράφει όλα τα πακέτα της συγκεκριμένης διεπαφής/κατεύθυνσης.

Η ενότητα των Εξερχομένων (Outbound) στο ακόλουθο σύνολο κανόνων, περιέχει μόνο κανόνες τύπου `pass` οι οποίοι επιτρέπουν (μέσω κατάλληλων τιμών στις παραμέτρους τους) σε

συγκεκριμένες υπηρεσίες να αποκτήσουν πρόσβαση στο Internet. Όλοι οι κανόνες διαθέτουν τις επιλογές `quick`, `on`, `proto`, `port` και `keep state`. Οι κανόνες `proto tcp` περιλαμβάνουν την επιλογή `flag` ώστε να αναγνωρίζουν την αίτηση έναρξης της συνεδρίας και να ενεργοποιούν τη λειτουργία διατήρησης της κατάστασης (stateful).

Στην ενότητα των εισερχόμενων πακέτων (Inbound) που φαίνεται παρακάτω, πρώτοι εμφανίζονται οι κανόνες που χρησιμοποιούνται για την απόρριψη των ανεπιθύμητων πακέτων. Αυτό γίνεται για δύο διαφορετικούς λόγους. Ο πρώτος είναι ότι τα κακόβουλα πακέτα μπορεί εν μέρει να ταιριάζουν με κάποια χαρακτηριστικά της έγκυρης κίνησης. Τα πακέτα αυτά θα πρέπει να απορριφθούν, αντί να γίνουν δεκτά από κάποιο επόμενο κανόνα `allow`. Ο δεύτερος είναι ότι μπορείτε να απορρίψετε συγκεκριμένα πακέτα τα οποία γνωρίζετε ότι δεν είναι έγκυρα, αλλά σας είναι αδιάφορη η καταγραφή τους. Με τον τρόπο αυτό εμποδίζεται η λήψη και καταγραφή τους από τον τελευταίο κανόνα. Ο τελευταίος κανόνας τυπικά απορρίπτει και καταγράφει όλα τα πακέτα που έφτασαν μέχρι αυτόν. Ο κανόνας αυτός χρησιμοποιείται για την παροχή νομικών αποδείξεων σε περίπτωση που κινήσετε δικαστική διαδικασία κατά ατόμων που προέβησαν σε επιθέσεις στο σύστημα σας.

Θα πρέπει επίσης να εξασφαλίσετε ότι το σύστημα σας δεν θα δώσει καμιά απάντηση σε κανένα από τα ανεπιθύμητα πακέτα. Τα πακέτα αυτά θα πρέπει να απορριφθούν και να εξαφανιστούν. Με τον τρόπο αυτό, ο επιτιθέμενος δεν έχει καμιά γνώση αν τα πακέτα του έφτασαν μέχρι το σύστημα σας. Όσο λιγότερα μπορούν να μάθουν οι επιτιθέμενοι σχετικά με το σύστημα σας, τόσο περισσότερο χρόνο θα χρειαστεί να επενδύσουν για να καταφέρουν να σας βλάψουν στα αλήθεια. Οι κανόνες με την επιλογή `log first` καταγράφουν το συμβάν μόνο την πρώτη φορά που ενεργοποιούνται. Η επιλογή αυτή περιλαμβάνεται στον κανόνα `nmap OS fingerprint` στο παράδειγμα που φαίνεται παρακάτω. Το βοηθητικό πρόγραμμα security/nmap χρησιμοποιείται συχνά από κακόβουλα άτομα, που προσπαθούν με αυτό τον τρόπο να αναγνωρίσουν το λειτουργικό σύστημα του μηχανήματος σας.

Κάθε φορά που υπάρχει καταγραφή από κάποιο κανόνα με την επιλογή `log first`, θα πρέπει να εκτελέσετε την εντολή `ipfstat -hio` για να δείτε πόσες φορές έχει ενεργοποιηθεί αυτός ο κανόνας συνολικά. Έτσι θα ξέρετε αν π.χ. σας κάνουν επίθεση υπερχείλισης (flood).

Δείτε το αρχείο /etc/services για να βρείτε αριθμούς θυρών που δεν αναγνωρίζετε. Μπορείτε επίσης να επισκεφθείτε την τοποθεσία http://www.securitystats.com/tools/portsearch.php και να κάνετε αναζήτηση για τη συγκεκριμένη θύρα, ώστε να δείτε ποια υπηρεσία εξυπηρετεί.

Δείτε την επόμενη τοποθεσία για τις θύρες που χρησιμοποιούνται συνήθως από κακόβουλα προγράμματα (trojans): http://www.simovits.com/trojans/trojans.html.

Το παρακάτω σύνολο κανόνων είναι αρκετά πλήρες και πολύ ασφαλές. Δημιουργεί firewall τύπου `inclusive`, και έχει δοκιμαστεί σε πραγματικές συνθήκες λειτουργίας. Μπορεί να εξυπηρετήσει το ίδιο καλά και το δικό σας σύστημα. Απλώς μετατρέψτε σε σχόλιο τους κανόνες για τις υπηρεσίες που δεν θέλετε να ενεργοποιήσετε.

Για να αποφύγετε την καταγραφή ανεπιθύμητων μηνυμάτων, απλώς προσθέστε ένα αντίστοιχο κανόνα απόρριψης (`block`) στην ενότητα των εισερχομένων (inbound).

Θα πρέπει να αλλάξετε το όνομα της διεπαφής dc0 του παραδείγματος, με το πραγματικό όνομα της κάρτας δικτύου που συνδέει το σύστημα σας με το Internet. Για όσους χρησιμοποιούν το PPP χρήστη, το όνομα θα είναι tun0.

Προσθέστε τις ακόλουθες καταχωρίσεις στο αρχείο /etc/ipf.rules:

```
#####################################################################
# No restrictions on Inside LAN Interface for private network
# Not needed unless you have LAN
#####################################################################

#pass out quick on xl0 all
#pass in quick on xl0 all

#####################################################################
# No restrictions on Loopback Interface
#####################################################################
pass in quick on lo0 all
pass out quick on lo0 all

#####################################################################
# Interface facing Public Internet (Outbound Section)
# Match session start requests originating from behind the
# firewall on the private network
# or from this gateway server destined for the public Internet.
#####################################################################

# Allow out access to my ISP's Domain name server.
# xxx must be the IP address of your ISP's DNS.
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
pass out quick on dc0 proto tcp from any to xxx port = 53 flags S keep state
pass out quick on dc0 proto udp from any to xxx port = 53 keep state

# Allow out access to my ISP's DHCP server for cable or DSL networks.
# This rule is not needed for 'user ppp' type connection to the
# public Internet, so you can delete this whole group.
# Use the following rule and check log for IP address.
# Then put IP address in commented out rule & delete first rule
pass out log quick on dc0 proto udp from any to any port = 67 keep state
#pass out quick on dc0 proto udp from any to z.z.z.z port = 67 keep state

# Allow out non-secure standard www function
pass out quick on dc0 proto tcp from any to any port = 80 flags S keep state

# Allow out secure www function https over TLS SSL
pass out quick on dc0 proto tcp from any to any port = 443 flags S keep state

# Allow out send & get email function
pass out quick on dc0 proto tcp from any to any port = 110 flags S keep state
pass out quick on dc0 proto tcp from any to any port = 25 flags S keep state

# Allow out Time
pass out quick on dc0 proto tcp from any to any port = 37 flags S keep state
```

```
# Allow out nntp news
pass out quick on dc0 proto tcp from any to any port = 119 flags S keep state

# Allow out gateway & LAN users' non-secure FTP ( both passive & active modes)
# This function uses the IPNAT built in FTP proxy function coded in
# the nat rules file to make this single rule function correctly.
# If you want to use the pkg_add command to install application packages
# on your gateway system you need this rule.
pass out quick on dc0 proto tcp from any to any port = 21 flags S keep state

# Allow out ssh/sftp/scp (telnet/rlogin/FTP replacements)
# This function is using SSH (secure shell)
pass out quick on dc0 proto tcp from any to any port = 22 flags S keep state

# Allow out insecure Telnet
pass out quick on dc0 proto tcp from any to any port = 23 flags S keep state

# Allow out FreeBSD CVSup function
pass out quick on dc0 proto tcp from any to any port = 5999 flags S keep state

# Allow out ping to public Internet
pass out quick on dc0 proto icmp from any to any icmp-type 8 keep state

# Allow out whois from LAN to public Internet
pass out quick on dc0 proto tcp from any to any port = 43 flags S keep state

# Block and log only the first occurrence of everything
# else that's trying to get out.
# This rule implements the default block
block out log first quick on dc0 all

######################################################################
# Interface facing Public Internet (Inbound Section)
# Match packets originating from the public Internet
# destined for this gateway server or the private network.
######################################################################

# Block all inbound traffic from non-routable or reserved address spaces
block in quick on dc0 from 192.168.0.0/16 to any    #RFC 1918 private IP
block in quick on dc0 from 172.16.0.0/12 to any     #RFC 1918 private IP
block in quick on dc0 from 10.0.0.0/8 to any        #RFC 1918 private IP
block in quick on dc0 from 127.0.0.0/8 to any       #loopback
block in quick on dc0 from 0.0.0.0/8 to any         #loopback
block in quick on dc0 from 169.254.0.0/16 to any    #DHCP auto-config
block in quick on dc0 from 192.0.2.0/24 to any      #reserved for docs
block in quick on dc0 from 204.152.64.0/23 to any   #Sun cluster interconnect
block in quick on dc0 from 224.0.0.0/3 to any       #Class D & E multicast

##### Block a bunch of different nasty things. ############
# That I do not want to see in the log
```

```
# Block frags
block in quick on dc0 all with frags

# Block short tcp packets
block in quick on dc0 proto tcp all with short

# block source routed packets
block in quick on dc0 all with opt lsrr
block in quick on dc0 all with opt ssrr

# Block nmap OS fingerprint attempts
# Log first occurrence of these so I can get their IP address
block in log first quick on dc0 proto tcp from any to any flags FUP

# Block anything with special options
block in quick on dc0 all with ipopts

# Block public pings
block in quick on dc0 proto icmp all icmp-type 8

# Block ident
block in quick on dc0 proto tcp from any to any port = 113

# Block all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
block in log first quick on dc0 proto tcp/udp from any to any port = 137
block in log first quick on dc0 proto tcp/udp from any to any port = 138
block in log first quick on dc0 proto tcp/udp from any to any port = 139
block in log first quick on dc0 proto tcp/udp from any to any port = 81

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type. Only necessary for
# cable or DSL configurations. This rule is not needed for
# 'user ppp' type connection to the public Internet.
# This is the same IP address you captured and
# used in the outbound section.
pass in quick on dc0 proto udp from z.z.z.z to any port = 68 keep state

# Allow in standard www function because I have apache server
pass in quick on dc0 proto tcp from any to any port = 80 flags S keep state

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID/PW passed over public Internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
#pass in quick on dc0 proto tcp from any to any port = 23 flags S keep state

# Allow in secure FTP, Telnet, and SCP from public Internet
# This function is using SSH (secure shell)
```

```
pass in quick on dc0 proto tcp from any to any port = 22 flags S keep state

# Block and log only first occurrence of all remaining traffic
# coming into the firewall. The logging of only the first
# occurrence avoids filling up disk with Denial of Service logs.
# This rule implements the default block.
block in log first quick on dc0 all
################### End of rules file ######################################
```

55.5.14. NAT

Το NAT είναι ακρωνύμιο των λέξεων *Network Address Translation* ή Μετάφραση Διευθύνσεων Δικτύου. Για όσους είναι εξοικειωμένοι με το Linux®, βασίζεται στην αρχή του IP Masquerading. Στην πραγματικότητα το NAT και το IP Masquerading είναι το ίδιο πράγμα. Μια από τις πολλές δυνατότητες που παρέχει η λειτουργία NAT του IPF, είναι και η δυνατότητα να έχουμε ένα ιδιωτικό τοπικό δίκτυο (LAN) πίσω από το firewall το οποίο να μοιράζεται μια μοναδική δημόσια διεύθυνση IP στο Internet.

Ίσως να αναρωτηθείτε γιατί να θέλει κάποιος να το κάνει αυτό. Οι ISPs συνήθως αποδίδουν δυναμικές διευθύνσεις σε μη εταιρικούς πελάτες. Αυτό ουσιαστικά σημαίνει ότι η διεύθυνση IP που αποδίδεται στο μηχάνημα σας, μπορεί να είναι διαφορετική κάθε φορά που κάνετε κλήση για να συνδεθείτε. Για τους χρήστες DSL modem και router, η αλλαγή διεύθυνσης πραγματοποιείται κάθε φορά που ενεργοποιείται το modem. Η διεύθυνση IP που σας αποδίδεται από τον ISP σας, είναι αυτή με την οποία φαίνεστε στο Internet.

Ας υποθέσουμε τώρα ότι έχετε πέντε PC στο σπίτι σας, και χρειάζεστε σε όλα σύνδεση Internet. Κανονικά, θα έπρεπε να πληρώσετε τον ISP σας χωριστό λογαριασμό για κάθε PC και να διαθέτετε πέντε γραμμές τηλεφώνου.

Με το NAT, χρειάζεστε μόνο ένα λογαριασμό με τον ISP σας. Μπορείτε απλώς να συνδέσετε τα τέσσερα PC σε ένα διανομέα ή switch στο οποίο θα συνδέσετε επίσης και το FreeBSD μηχάνημα σας. Το μηχάνημα αυτό θα ενεργεί ως πύλη του τοπικού σας δικτύου για το Internet. Το NAT θα μεταφράσει αυτόματα τις ιδιωτικές διευθύνσεις IP του κάθε μηχανήματος στην μοναδική δημόσια IP διεύθυνση που έχετε, καθώς το πακέτο φεύγει από το firewall και κατευθύνεται προς το Internet. Εκτελεί επίσης και την αντίστροφη μετάφραση για τα πακέτα που επιστρέφουν.

Υπάρχει μια ειδική περιοχή διευθύνσεων IP που έχουν παραχωρηθεί για χρήση σε τοπικά δίκτυα με NAT. Σύμφωνα με το RFC 1918, μπορείτε να χρησιμοποιήσετε για αυτό το σκοπό τις παρακάτω περιοχές, οι οποίες δεν δρομολογούνται ποτέ απευθείας στο δημόσιο Internet:

Αρχικό IP `10.0.0.0`	-	Τελικό IP `10.255.255.255`
Αρχικό IP `172.16.0.0`	-	Τελικό IP `172.31.255.255`
Αρχικό IP `192.168.0.0`	-	Τελικό IP `192.168.255.255`

55.5.15. IPNAT

Οι κανόνες του NAT φορτώνονται με τη χρήση της εντολής `ipnat`. Τυπικά, οι κανόνες του NAT αποθηκεύονται στο αρχείο /etc/ipnat.rules. Δείτε τη σελίδα manual του ipnat(1) για λεπτομέρειες.

Για να αλλάξετε τους κανόνες του NAT καθώς αυτό εκτελείται, τροποποιήστε το αρχείο που τους περιέχει, και εκτελέστε την εντολή `ipnat` με την παράμετρο `-CF` για να διαγράψετε τους εσωτερικούς κανόνες του NAT και να αδειάσετε όλες τις ενεργές καταχωρίσεις του πίνακα μεταφράσεων.

Για να φορτώσετε τους κανόνες του NAT από την αρχή, εκτελέστε μια εντολή όπως την παρακάτω:

```
# ipnat -CF -f /etc/ipnat.rules
```

Για να δείτε κάποια στατιστικά σχετικά με το NAT, χρησιμοποιήστε την παρακάτω εντολή:

```
# ipnat -s
```

Για να δείτε μια λίστα με τις τρέχουσες καταχωρίσεις του πίνακα NAT, χρησιμοποιήστε την παρακάτω εντολή:

```
# ipnat -l
```

Για να ενεργοποιήσετε την λεπτομερή απεικόνιση μηνυμάτων και να δείτε πληροφορίες που σχετίζονται με την επεξεργασία των κανόνων και τους ενεργούς κανόνες και καταχωρίσεις στον πίνακα, γράψτε:

```
# ipnat -v
```

55.5.16. Κανόνες του IPNAT

Οι κανόνες του NAT είναι αρκετά ευέλικτοι, και διαθέτουν πλήθος δυνατοτήτων ώστε να καλύπτουν τις ανάγκες των οικιακών αλλά και των επιχειρησιακών χρηστών.

Η σύνταξη των κανόνων που παρουσιάζεται εδώ, έχει απλοποιηθεί ώστε να συμβαδίζει με τη συνήθη χρήση σε μη-εμπορικά περιβάλλοντα. Για πιο πλήρη περιγραφή της σύνταξης, δείτε τη σελίδα manual του ipnat(5).

Η σύνταξη ενός κανόνα NAT μοιάζει με την παρακάτω:

```
map IF LAN_IP_RANGE -> PUBLIC_ADDRESS
```

Ο κανόνας ξεκινάει με τη λέξη `map`.

Αντικαταστήστε το *IF* με την εξωτερική διεπαφή (τη κάρτα δικτύου που συνδέεται στο Internet).

Η παράμετρος `LAN_IP_RANGE` είναι η περιοχή διευθύνσεων που χρησιμοποιείται από το εσωτερικό σας δίκτυο. Στην πραγματικότητα θα μοιάζει με κάτι σαν το `192.168.1.0/24`.

Η παράμετρος `PUBLIC_ADDRESS` μπορεί να είναι είτε η εξωτερική IP διεύθυνση, είτε η ειδική λέξη `0/32`, η οποία σημαίνει ότι θα χρησιμοποιηθεί η IP διεύθυνση που έχει αποδοθεί στο *IF*.

55.5.17. Πως Λειτουργεί το NAT

Ένα πακέτο φτάνει στο firewall από το LAN με προορισμό το Internet. Περνάει διαμέσου των κανόνων φιλτραρίσματος εξερχομένων, όπου γίνεται η επεξεργασία του από το NAT. Οι κανόνες εφαρμόζονται από τον πρώτο και προς τα κάτω, και κερδίζει ο πρώτος που ταιριάζει. Ο έλεγχος γίνεται με βάση τη διεπαφή από την οποία λήφθηκε το πακέτο και τη διεύθυνση IP από την οποία προέρχεται. Όταν το όνομα της διεπαφής ενός πακέτου ταιριάζει με κάποιο κανόνα του NAT, η διεύθυνση IP της αφετηρίας (που προέρχεται από το ιδιωτικό δίκτυο) ελέγχεται για να εξακριβωθεί αν ταιριάζει με την περιοχή διευθύνσεων που καθορίζεται στην αριστερά πλευρά του συμβόλου (βέλος) του κανόνα NAT. Αν ταιριάζει, η διεύθυνση του πακέτου ξαναγράφεται, χρησιμοποιώντας τη δημόσια διεύθυνση IP η οποία παρέχεται από το `0/32`. Το NAT δημιουργεί μια καταχώριση στον εσωτερικό του πίνακα, έτσι ώστε όταν επιστρέψει η απάντηση από το Internet, να μπορεί να αντιστοιχηθεί ξανά στην αρχική ιδιωτική διεύθυνση IP και να περάσει έπειτα από τους κανόνες του φίλτρου για περαιτέρω επεξεργασία.

55.5.18. Ενεργοποιώντας το IPNAT

Για να ενεργοποιήσετε το IPNAT, προσθέστε τις παρακάτω γραμμές στο /etc/rc.conf.

Για να επιτρέψετε στο μηχάνημα σας να δρομολογεί πακέτα μεταξύ διεπαφών δικτύου:

```
gateway_enable="YES"
```

Για να ξεκινάει αυτόματα το IPNAT σε κάθε εκκίνηση:

```
ipnat_enable="YES"
```

Για να καθορίσετε από που επιθυμείτε να φορτώνονται οι κανόνες του IPNAT:

```
ipnat_rules="/etc/ipnat.rules"
```

55.5.19. Το NAT σε Ένα Μεγάλο Τοπικό Δίκτυο

Για τοπικά δίκτυα με μεγάλο αριθμό υπολογιστών, ή για δίκτυα που διασυνδέουν περισσότερα από ένα LAN, η διαδικασία της μετατροπής όλων αυτών των ιδιωτικών διευθύνσεων σε μια μοναδική δημόσια διεύθυνση, δημιουργεί πρόβλημα κατανομής πόρων, καθώς χρησιμοποιούνται πολλές φορές οι ίδιοι αριθμοί θυρών, οδηγώντας τα PC του δικτύου σε συγκρούσεις. Υπάρχουν δύο τρόποι για να ελαττώσουμε αυτό το πρόβλημα.

55.5.19.1. Ανάθεση των θυρών που θα Χρησιμοποιηθούν

Ένα συνηθισμένος κανόνας NAT μοιάζει με τον παρακάτω:

```
map dc0 192.168.1.0/24 -> 0/32
```

Στον παραπάνω κανόνα, η θύρα αφετηρίας του πακέτου παραμένει αναλλοίωτη καθώς το πακέτο διέρχεται μέσω του IPNAT. Αν προσθέσετε την λέξη-κλειδί `portmap`, μπορείτε να ρυθμίσετε το IPNAT να χρησιμοποιεί θύρες που ανήκουν σε μια καθορισμένη περιοχή. Για παράδειγμα, ο παρακάτω κανόνας θα οδηγήσει το NAT να τροποποιήσει την θύρα της αφετηρίας, ώστε να είναι μέσα στην περιοχή που φαίνεται:

```
map dc0 192.168.1.0/24 -> 0/32 portmap tcp/udp 20000:60000
```

Μπορούμε επίσης να απλοποιήσουμε ακόμα περισσότερο τη διαδικασία χρησιμοποιώντας τη λέξη `auto` ώστε το IPNAT να καθορίζει από μόνο του ποιες θύρες είναι διαθέσιμες για χρήση:

```
map dc0 192.168.1.0/24 -> 0/32 portmap tcp/udp auto
```

55.5.19.2. Χρησιμοποιώντας ένα Απόθεμα Δυναμικών Διευθύνσεων

Σε ένα πολύ μεγάλο τοπικό δίκτυο, αργά ή γρήγορα φτάνουμε στο σημείο που μια μοναδική δημόσια διεύθυνση δεν επαρκεί για να καλύψει τόσες πολλές ιδιωτικές. Αν υπάρχει διαθέσιμο ένα εύρος δημοσίων διευθύνσεων, μπορούν να χρησιμοποιηθούν ως "απόθεμα (pool)", επιτρέποντας στην IPNAT να επιλέξει μια από αυτές καθώς αντιστοιχεί τα πακέτα κατά την έξοδο τους προς το δημόσιο δίκτυο.

Για παράδειγμα, αντί να αντιστοιχούν όλα τα πακέτα μέσω μιας μοναδικής δημόσιας IP διεύθυνσης όπως παρακάτω:

```
map dc0 192.168.1.0/24 -> 204.134.75.1
```

μπορούμε να χρησιμοποιήσουμε ένα εύρος IP διευθύνσεων, είτε με τη χρήση μάσκας δικτύου:

```
map dc0 192.168.1.0/24 -> 204.134.75.0/255.255.255.0
```

είτε με συμβολισμό CIDR:

```
map dc0 192.168.1.0/24 -> 204.134.75.0/24
```

55.5.20. Ανακατεύθυνση Θυρών

Είναι κοινή πρακτική να εγκαθίστανται υπηρεσίες όπως ο εξυπηρετητής ιστοσελίδων, ταχυδρομείου, βάσης δεδομένων και DNS σε διαφορετικά PC στο τοπικό δίκτυο. Στην περίπτωση αυτή, η κίνηση πακέτων από αυτά τα μηχανήματα εξακολουθεί να χρειάζεται το NAT, αλλά χρειάζεται επίσης να υπάρχει κάποιος τρόπος να κατευθύνεται η εισερχόμενη κίνηση στα σωστά PC του δικτύου. Το IPNAT έχει τις κατάλληλες δυνατότητες για την επίλυση αυτού του προβλήματος. Για παράδειγμα, έστω ότι ένας εξυπηρετητής ιστοσελίδων βρίσκεται στην διεύθυνση LAN `10.0.10.25` και η μοναδική δημόσια IP είναι `20.20.20.5`. Ο κανόνας που θα γράφατε θα έμοιαζε με τον παρακάτω:

```
rdr dc0 20.20.20.5/32 port 80 -> 10.0.10.25 port 80
```

ή:

```
rdr dc0 0.0.0.0/0 port 80 -> 10.0.10.25 port 80
```

ή για ένα εξυπηρετητή DNS με διεύθυνση στο τοπικό δίκτυο `10.0.10.33` ο οποίος πρέπει να δέχεται αναζητήσεις από το δημόσιο δίκτυο:

```
rdr dc0 20.20.20.5/32 port 53 -> 10.0.10.33 port 53 udp
```

55.5.21. FTP και NAT

Το FTP είναι ένας δεινόσαυρος που έχει απομείνει από την εποχή που το Internet ήταν στα αρχικά του στάδια, όπου τα ερευνητικά εργαστήρια των πανεπιστήμιων ήταν συνδεμένα μεταξύ τους με μισθωμένες γραμμές και οι ερευνητές το χρησιμοποιούσαν για να στέλνουν αρχεία ο ένας στον άλλο. Την εποχή εκείνη, δεν υπήρχαν ανησυχίες σχετικά με την ασφάλεια. Με το πέρασμα του χρόνου, το FTP θάφτηκε στο πίσω μέρος του ταχέως εξελισσόμενου Internet. Δεν εξελίχθηκε ποτέ ώστε να ξεπεράσει προβλήματα ασφάλειας, όπως π.χ. το γεγονός ότι στέλνει το όνομα και τον κωδικό του χρήστη ως απλό κείμενο. Το FTP έχει δυο καταστάσεις λειτουργίας, την ενεργή και την παθητική. Η διαφορά είναι στο πως γίνεται η ανάκτηση του καναλιού δεδομένων. Η παθητική λειτουργία είναι πιο ασφαλής, καθώς το κανάλι δεδομένων αποτελεί το κύριο κανάλι της συνεδρίας. Μπορείτε να βρείτε πολύ καλή περιγραφή του πρωτοκόλλου και των διαφορετικών τρόπων λειτουργίας του, στο http://www.slacksite.com/other/ftp.html.

55.5.21.1. Κανόνες του IPNAT

Το IPNAT διαθέτει μια ειδική επιλογή για διαμεσολάβηση FTP (proxy) η οποία μπορεί να καθοριστεί στον κατάλληλο κανόνα του NAT. Μπορεί να παρακολουθήσει όλα τα εξερχόμενα πακέτα για να ανιχνεύσει την έναρξη μιας ενεργής ή παθητικής συνεδρίας FTP, και να δημιουργήσει δυναμικά προσωρινούς κανόνες στο φίλτρο που να περιέχουν μόνο τον αριθμό της θύρας που χρησιμοποιείται από το κανάλι δεδομένων. Αυτό εξαλείφει το πρόβλημα ασφάλειας που δημιουργείται από το γεγονός ότι διαφορετικά θα χρειαζόταν να ανοιχθεί μια μεγάλη περιοχή θυρών (στην υψηλή περιοχή) στο firewall.

Ο παρακάτω κανόνας χειρίζεται όλα τα δεδομένα για το εσωτερικό δίκτυο (LAN):

```
map dc0 10.0.10.0/29 -> 0/32 proxy port 21 ftp/tcp
```

Ο παρακάτω κανόνας χειρίζεται την κίνηση FTP από την πύλη (gateway):

```
map dc0 0.0.0.0/0 -> 0/32 proxy port 21 ftp/tcp
```

Ο παρακάτω κανόνας χειρίζεται όλη την κίνηση από το εσωτερικό LAN που δεν ανήκει στο

πρωτόκολλο FTP:

```
map dc0 10.0.10.0/29 -> 0/32
```

Ο κανόνας χαρτογράφησης του FTP τοποθετείται πριν από τον κανονικό κανόνα χαρτογράφησης. Κάθε πακέτο ελέγχεται αρχικά από τον κανόνα που βρίσκεται στην κορυφή. Αν ταιριάζει στη διεπαφή και στην ιδιωτική διεύθυνση IP και πρόκειται για πακέτο FTP, ο διαμεσολαβητής FTP δημιουργεί προσωρινούς κανόνες στο φίλτρο οι οποίοι επιτρέπουν την εισερχόμενη και εξερχόμενη κίνηση FTP ενώ ταυτόχρονα εκτελούν και την απαραίτητη μετάφραση NAT. Όλα τα πακέτα που δεν ανήκουν σε μετάδοση FTP δεν ταιριάζουν με τον πρώτο κανόνα, έτσι κατευθύνονται στον τρίτο κανόνα, εξετάζονται όσο αφορά τη διεπαφή και το IP από το οποίο προέρχονται, και γίνεται η αντίστοιχη μετάφραση τους από το NAT.

55.5.21.2. Κανόνες Φίλτρου για το IPNAT

Όταν χρησιμοποιείται ο μεσολαβητής FTP, χρειάζεται μόνο ένας κανόνας για το NAT.

Χωρίς το μεσολαβητή FTP, χρειάζονται οι παρακάτω τρεις κανόνες:

```
# Allow out LAN PC client FTP to public Internet
# Active and passive modes
pass out quick on rl0 proto tcp from any to any port = 21 flags S keep state

# Allow out passive mode data channel high order port numbers
pass out quick on rl0 proto tcp from any to any port > 1024 flags S keep state

# Active mode let data channel in from FTP server
pass in quick on rl0 proto tcp from any to any port = 20 flags S keep state
```

55.6. IPFW

Το IPFIREWALL (IPFW) είναι λογισμικό που αναπτύχθηκε για το FreeBSD. Έχει γραφεί και συντηρείται από εθελοντές που ανήκουν στο Project. Χρησιμοποιεί τους κλασικούς κανόνες χωρίς διατήρηση της κατάστασης (stateless) καθώς και μια τεχνική κωδικοποίησης που επιτυγχάνει αυτό που αναφέρεται ως Απλή Stateful Λογική (Simple Stateful Logic).

Το υπόδειγμα κανόνων για το IPFW (στα αρχεία /etc/rc.firewall και /etc/rc.firewall6) της τυπικής εγκατάστασης του FreeBSD είναι μάλλον απλό και θα χρειαστεί να κάνετε κάποιες αλλαγές πριν το χρησιμοποιήσετε. Το παράδειγμα δεν χρησιμοποιεί φιλτράρισμα τύπου stateful. Η stateful λειτουργία είναι ευεργετική στις περισσότερες περιπτώσεις, έτσι δεν θα χρησιμοποιήσουμε αυτό το παράδειγμα ως βάση αυτής της ενότητας.

Η σύνταξη των κανόνων stateless του IPFW έχει ενισχυθεί με εξελιγμένες δυνατότητες επιλογής οι οποίες συνήθως ξεπερνάνε κατά πολύ τις τυπικές γνώσεις του ατόμου που καλείται να το ρυθμίσει. Το IPFW απευθύνεται στον επαγγελματία χρήστη ή τον τεχνικά προχωρημένο χομπίστα, ο οποίος έχει ανάγκη προχωρημένου φιλτραρίσματος πακέτων. Η πραγματική δύναμη των κανόνων του IPFW αποκαλύπτεται μόνο αν διαθέτετε προχωρημένες γνώσεις σχετικά με το πως διαφορετικά

πρωτόκολλα δημιουργούν και χρησιμοποιούν την επικεφαλίδα των πακέτων τους. Τέτοιο επίπεδο επεξηγήσεων είναι πέρα από το σκοπό αυτής της ενότητας του Εγχειριδίου.

Το IPFW αποτελείται από επτά εξαρτήματα. Το βασικό εξάρτημα είναι ο επεξεργαστής κανόνων του firewall στον πυρήνα, με ενσωματωμένη τη δυνατότητα καταγραφής. Τα υπόλοιπα εξαρτήματα είναι το σύστημα καταγραφής (logging), ο κανόνας `divert` ο οποίος ενεργοποιεί τη λειτουργία NAT, καθώς και οι προχωρημένες δυνατότητες ειδικού σκοπού: το σύστημα διαμόρφωσης κίνησης (traffic shaper) dummynet, η δυνατότητα προώθησης μέσω του `fwd rule`, η δυνατότητα γεφύρωσης (bridge) καθώς και η δυνατότητα απόκρυψης (ipstealth). Το IPFW υποστηρίζει τόσο το πρωτόκολλο IPv4 όσο και το IPv6.

55.6.1. Ενεργοποιώντας το IPFW

Το IPFW περιλαμβάνεται στην βασική εγκατάσταση του FreeBSD ως άρθρωμα του πυρήνα το οποίο μπορεί να φορτωθεί δυναμικά. Το σύστημα θα φορτώσει δυναμικά το άρθρωμα όταν βρει την καταχώριση `firewall_enable="YES"` στο αρχείο /etc/rc.conf. Δεν χρειάζεται να μεταγλωττίσετε το IPFW μέσα στον πυρήνα.

Αφού επανεκκινήσετε το σύστημα σας με την καταχώριση `firewall_enable="YES"` στο rc.conf, θα δείτε με άσπρα έντονα γράμματα το ακόλουθο μήνυμα κατά τη διαδικασία της εκκίνησης:

```
ipfw2 initialized, divert disabled, rule-based forwarding disabled, default to deny,
logging disabled
```

Το άρθρωμα έχει ενσωματωμένη τη δυνατότητα καταγραφής. Για να ενεργοποιήσετε την καταγραφή και να θέσετε το επίπεδο λεπτομέρειας, υπάρχουν κάποιες ρυθμίσεις που μπορείτε να θέσετε στο /etc/sysctl.conf. Προσθέτοντας τις παρακάτω καταχωρίσεις, θα ενεργοποιηθεί η καταγραφή στις επόμενες εκκινήσεις:

```
net.inet.ip.fw.verbose=1
net.inet.ip.fw.verbose_limit=5
```

55.6.2. Επιλογές του Πυρήνα

Δεν είναι υποχρεωτικό να ενεργοποιήσετε το IPFW μεταγλωττίζοντας τις παρακάτω επιλογές στον πυρήνα του FreeBSD. Ο σκοπός αυτής της παρουσίασης είναι καθαρά ενημερωτικός.

```
options    IPFIREWALL
```

Η επιλογή αυτή ενεργοποιεί το IPFW ως μέρος του πυρήνα.

```
options    IPFIREWALL_VERBOSE
```

Ενεργοποιεί την καταγραφή των πακέτων που περνούν μέσω του IPFW και περιλαμβάνουν τη λέξη `log` στον κανόνα τους.

```
options    IPFIREWALL_VERBOSE_LIMIT=5
```

Περιορίζει τον πλήθος των πακέτων που καταγράφονται μέσω του syslogd(8) σε συγκεκριμένο αριθμό ανά καταχώριση. Η ρύθμιση είναι χρήσιμη σε εχθρικά περιβάλλοντα στα οποία είναι επιθυμητή η καταγραφή. Με αυτό τον τρόπο μπορεί να αποφευχθεί μια πιθανή επίθεση με στόχο την υπερχείλιση των αρχείων καταγραφής.

```
options    IPFIREWALL_DEFAULT_TO_ACCEPT
```

Η επιλογή αυτή αφήνει τα πάντα να περνάνε μέσα από το firewall, το οποίο είναι καλή ιδέα την πρώτη φορά που ρυθμίζετε το firewall σας.

```
options    IPDIVERT
```

Η επιλογή αυτή ενεργοποιεί τη λειτουργία NAT.

Το firewall θα απορρίπτει όλα τα πακέτα που κατευθύνονται από και προς το μηχάνημα, αν δεν περιλάβετε την επιλογή `IPFIREWALL_DEFAULT_TO_ACCEPT` ή αν δεν ρυθμίσετε ένα κατάλληλο κανόνα που να επιτρέπει αυτές τις συνδέσεις.

55.6.3. Επιλογές στο /etc/rc.conf

Ενεργοποιήστε το firewall:

```
firewall_enable="YES"
```

Για να επιλέξετε ένα από τους προεπιλεγμένους τύπους firewall που υποστηρίζονται από το FreeBSD, διαβάστε το αρχείο /etc/rc.firewall και δημιουργήστε μια εγγραφή όπως την παρακάτω:

```
firewall_type="open"
```

Οι διαθέσιμες τιμές για αυτή τη ρύθμιση είναι:

- `open` - επιτρέπει τη διέλευση όλης της κίνησης.
- `client` - προστατεύει μόνο το συγκεκριμένο μηχάνημα.
- `simple` - προστατεύει ολόκληρο το δίκτυο.
- `closed` - απενεργοποιεί εντελώς την κίνηση πακέτων, εκτός από την εσωτερική διεπαφή (loopback).
- `UNKNOWN` - απενεργοποιεί την φόρτωση κανόνων του firewall.
- filename - το πλήρες μονοπάτι του αρχείου που περιέχει τους κανόνες του firewall.

Μπορείτε να χρησιμοποιήσετε δύο διαφορετικούς τρόπους για να φορτώσετε προσαρμοσμένους

κανόνες στο ipfw firewall. Ο ένας είναι θέτοντας τη μεταβλητή `firewall_type` στην απόλυτη διαδρομή του αρχείου που περιέχει τους *κανόνες του firewall*, χωρίς να δώσετε ορίσματα στην γραμμή εντολών για το ίδιο το ipfw(8). Το αρχείο κανόνων που φαίνεται παρακάτω, απορρίπτει όλη την εισερχόμενη και εξερχόμενη κίνηση:

```
add deny in
add deny out
```

Από την άλλη μεριά, είναι επίσης δυνατό να θέσετε τη μεταβλητή `firewall_script` στην απόλυτη διαδρομή ενός εκτελέσιμου script που περιλαμβάνει μια σειρά από εντολές `ipfw` που θα εκτελεστούν κατά την εκκίνηση. Ένα έγκυρο τέτοιο script το οποίο είναι αντίστοιχο με το αρχείο κανόνων που δείξαμε παραπάνω, είναι το ακόλουθο:

```
#!/bin/sh

ipfw -q flush

ipfw add deny in
ipfw add deny out
```

Αν θέσετε την τιμή του `firewall_type` είτε σε `client` είτε σε `simple`, θα πρέπει να ελέγξετε ότι οι προεπιλεγμένοι κανόνες που περιέχονται στο /etc/rc.firewall ταιριάζουν με τις ρυθμίσεις του συγκεκριμένου μηχανήματος. Παρατηρήστε επίσης ότι τα παραδείγματα που χρησιμοποιούνται σε αυτό το κεφάλαιο αναμένουν να να έχετε θέσει τη μεταβλητή `firewall_script` στην τιμή /etc/ipfw.rules.

Ενεργοποιήστε την καταγραφή:

```
firewall_logging="YES"
```

Το μόνο πράγμα που κάνει η μεταβλητή `firewall_logging` είναι να θέσει την τιμή της μεταβλητής sysctl `net.inet.ip.fw.verbose` στην τιμή `1` (δείτε το Ενεργοποιώντας το IPFW). Δεν υπάρχει μεταβλητή του rc.conf που να ορίζει περιορισμούς στην καταγραφή, αλλά αυτό μπορεί να ρυθμιστεί μέσω της παραπάνω μεταβλητής sysctl είτε χειροκίνητα, είτε μέσω του αρχείου /etc/sysctl.conf:

```
net.inet.ip.fw.verbose_limit=5
```

Αν το μηχάνημα σας λειτουργεί ως πύλη (gateway), δηλαδή παρέχει υπηρεσία μετάφρασης διευθύνσεων δικτύου (Network Address Translation, NAT) μέσω του natd(8), παρακαλούμε να διαβάσετε το Network Address Translation για πληροφορίες σχετικά με τις ρυθμίσεις που απαιτούνται στο αρχείο /etc/rc.conf.

55.6.4. Η Εντολή IPFW

Η εντολή `ipfw` είναι ο συνήθης τρόπος για την προσθήκη η διαγραφή κανόνων στους εσωτερικούς ενεργούς κανόνες του firewall, καθώς αυτό εκτελείται. Το πρόβλημα με τη χρήση αυτής της μεθόδου είναι ότι οι αλλαγές χάνονται με τον τερματισμό λειτουργίας του μηχανήματος. Μπορείτε να γράψετε όλους τους κανόνες σας σε ένα αρχείο και να το χρησιμοποιείτε για να τους φορτώνετε στην εκκίνηση. Μπορείτε να χρησιμοποιήσετε το ίδιο αρχείο για να αντικαταστήσετε τους τρέχοντες κανόνες του firewall, την ώρα που αυτό εκτελείται. Αυτός είναι και ο συνιστώμενος τρόπος που χρησιμοποιούμε στα παραδείγματα μας.

Η εντολή `ipfw` είναι επίσης χρήσιμη για να απεικονίζει τους τρέχοντες κανόνες στη κονσόλα σας. Το σύστημα καταγραφής χρήσης της IPFW δημιουργεί αυτόματα ένα μετρητή για κάθε κανόνα, ο οποίος μετράει πόσα πακέτα ταίριαξαν με αυτόν. Κατά τη διάρκεια των δοκιμών, η δυνατότητα να ελέγξετε την τιμή του μετρητή είναι ένας τρόπος για να διαπιστώσετε αν ο κανόνας λειτουργεί κανονικά.

Για να δείτε όλους τους κανόνες με τη σειρά:

```
# ipfw list
```

Για να δείτε μια λίστα όλων των κανόνων, μαζί με την ώρα που ενεργοποιήθηκε τελευταία φορά ο κάθε κανόνας, γράψτε:

```
# ipfw -t list
```

Το επόμενο παράδειγμα δείχνει τον αριθμό των πακέτων που ταίριαξαν μαζί με τον αντίστοιχο κανόνα. Η πρώτη στήλη δείχνει τον αριθμό του κανόνα, ακολουθείται από τον αριθμό πακέτων που ταίριαξαν (πρώτα τα εξερχόμενα και μετά τα εισερχόμενα) και τέλος από τον ίδιο τον κανόνα.

```
# ipfw -a list
```

Για να δείτε μια λίστα που να περιλαμβάνει τόσο τους δυναμικούς όσο και τους στατικούς κανόνες:

```
# ipfw -d list
```

Για να δείτε και τους δυναμικούς κανόνες που έχουν λήξει:

```
# ipfw -d -e list
```

Για να μηδενίσετε τους μετρητές:

```
# ipfw zero
```

Για να μηδενίσετε τους μετρητές μόνο για τον κανόνα με τον αριθμό *NUM*:

```
# ipfw zero NUM
```

55.6.5. Το Σύνολο Κανόνων του IPFW

Ως "σύνολο κανόνων" στο IPFW, ορίζουμε μια ομάδα κανόνων που έχουν γραφεί για να επιτρέπουν ή να απορρίπτουν πακέτα ανάλογα με τις τιμές που περιέχονται σε αυτά. Η διπλής κατεύθυνσης ανταλλαγή πακέτων μεταξύ υπολογιστών αποτελεί μια συνεδρία. Το σύνολο κανόνων του firewall επεξεργάζεται τόσο τα πακέτα που έρχονται από το Internet, όσο και τα πακέτα που παράγονται από το σύστημα ως απάντηση σε αυτά. Κάθε υπηρεσία TCP/IP (π.χ. telnet, www, mail, κ.λ.π.) καθορίζεται από το πρωτόκολλο και την προνομιακή (privileged) θύρα που χρησιμοποιεί για να δέχεται αιτήματα εξυπηρέτησης. Τα πακέτα που προορίζονται για μια συγκεκριμένη υπηρεσία, ξεκινούν από τη διεύθυνση αφετηρίας χρησιμοποιώντας μια μη-προνομιακή θύρα και καταλήγουν στη συγκεκριμένη θύρα υπηρεσίας στον προορισμό. Όλες οι παραπάνω παράμετροι (θύρες και διευθύνσεις) μπορούν να χρησιμοποιηθούν ως κριτήρια επιλογής για την δημιουργία κανόνων που επιτρέπουν ή εμποδίζουν την πρόσβαση σε υπηρεσίες.

Όταν ένα πακέτο εισέρχεται στο firewall, συγκρίνεται με βάση τον πρώτο κανόνα. Η σύγκριση συνεχίζεται διαδοχικά με τους υπόλοιπους κανόνες, από τον πρώτο προς τον τελευταίο, με βάση τον αύξοντα αριθμό τους. Όταν το πακέτο ταιριάξει με τις παραμέτρους επιλογής κάποιου κανόνα, εκτελείται η οδηγία που αναφέρεται στο πεδίο ενεργειών του κανόνα αυτού και η αναζήτηση κανόνων για το συγκεκριμένο πακέτο τερματίζεται. Σε αυτή τη μέθοδο αναζήτησης, "ο πρώτος κανόνας που ταιριάζει, είναι ο νικητής". Αν το πακέτο δεν ταιριάζει με κανένα από τους κανόνες, θα ληφθεί από τον υποχρεωτικό προεπιλεγμένο κανόνα του IPFW, με αριθμό 65535, ο οποίος εμποδίζει τη διέλευση όλων των πακέτων, και τα απορρίπτει χωρίς να στείλει καμιά απάντηση στον αρχικό αποστολέα τους.

Η αναζήτηση συνεχίζεται μετά από κανόνες τύπου `count`, `skipto` και `tee`.

Οι οδηγίες που φαίνονται εδώ, βασίζονται στη χρήση κανόνων που περιέχουν τις οδηγίες `keep state`, `limit`, `in`, `out` και `via`. Αυτές είναι και οι βασικές λειτουργίες για την δόμηση ενός firewall τύπου inclusive με stateful λειτουργία.

Να δίνετε μεγάλη προσοχή όταν δουλεύετε με τους κανόνες ενός firewall. Μπορεί άθελα σας να κλειδωθείτε έξω από το σύστημα σας.

55.6.5.1. Σύνταξη Κανόνων

Στην ενότητα αυτή, θα παρουσιάσουμε μια απλοποιημένη σύνταξη κανόνων. Δείχνουμε μόνο ότι χρειάζεται για να δημιουργηθεί ένα τυποποιημένο σύνολο κανόνων για ένα inclusive firewall. Για πλήρη περιγραφή, δείτε τη σελίδα manual του ipfw(8).

Οι κανόνες περιέχουν λέξεις-κλειδιά. Οι λέξεις αυτές θα πρέπει να κωδικοποιηθούν με συγκεκριμένη σειρά από τα αριστερά προς τα δεξιά της γραμμής. Οι λέξεις-κλειδιά φαίνονται παρακάτω με έντονα γράμματα. Μερικές λέξεις έχουν υπο-επιλογές οι οποίες μπορεί να είναι επίσης λέξεις-κλειδιά και να περιλαμβάνουν επίσης ακόμα περισσότερες υπο-επιλογές.

Η αρχή ενός σχολίου, σηματοδοτείται με το σύμβολο #, το οποίο μπορεί να εμφανίζεται στο τέλος μιας γραμμής κανόνα, ή και σε μια δική του γραμμή. Οι κενές γραμμές αγνοούνται.

```
CMD RULE_NUMBER ACTION LOGGING SELECTION STATEFUL
```

55.6.5.1.1. CMD

Για να γίνει η προσθήκη ενός νέου κανόνα στον εσωτερικό πίνακα, τοποθετείται μπροστά από αυτόν η παράμετρος add.

55.6.5.1.2. RULE_NUMBER

Κάθε κανόνας σχετίζεται με ένα αριθμό κανόνα (rule_number) στην περιοχή 1..65535.

55.6.5.1.3. ACTION

Ένας κανόνας μπορεί να σχετίζεται με μια ή περισσότερες ενέργειες, οι οποίες εκτελούνται όταν το πακέτο ταιριάζει με τα κριτήρια επιλογής αυτού του κανόνα.

allow | accept | pass | permit

Όλα τα παραπάνω έχουν το ίδιο αποτέλεσμα: το πακέτο εξέρχεται από την σύστημα του firewall. Η αναζήτηση για το συγκεκριμένο πακέτο τερματίζεται σε αυτό τον κανόνα.

check-state

Ελέγχει το πακέτο με βάση το δυναμικό πίνακα κανόνων. Αν βρεθεί κανόνας που να ταιριάζει, θα εκτελεστεί η ενέργεια του κανόνα ο οποίος δημιούργησε τον συγκεκριμένο δυναμικό κανόνα. Διαφορετικά, η αναζήτηση συνεχίζεται με τον επόμενο κανόνα. Ένας κανόνας check-state δεν έχει κριτήρια επιλογής. Αν δεν υπάρχει κανόνας check-state στο σύνολο κανόνων, ο έλεγχος του πίνακα δυναμικών κανόνων ξεκινάει από τον πρώτο κανόνα τύπου keep-state ή limit.

deny | drop

Και οι δύο λέξεις σημαίνουν το ίδιο πράγμα: τα πακέτα που ταιριάζουν με αυτό τον κανόνα απορρίπτονται. Η αναζήτηση τερματίζεται.

55.6.5.1.4. Καταγραφή

log ή logamount

Όταν ένα πακέτο ταιριάζει με ένα κανόνα που περιέχει τη λέξη `log`, γίνεται καταγραφή του μηνύματος μέσω του syslogd(8) στη δυνατότητα SECURITY. Η καταγραφή συμβαίνει μόνο αν ο αριθμός των πακέτων που έχει καταγραφεί μέχρι στιγμής δεν υπερβαίνει την παράμετρο `logamount`. Αν η παράμετρος αυτή δεν έχει καθοριστεί, το όριο ρυθμίζεται με βάση την τιμή της μεταβλητής sysctl `net.inet.ip.fw.verbose_limit`. Και στις δύο περιπτώσεις, μια μηδενική τιμή σημαίνει ότι δεν θα υπάρχει όριο στην καταγραφή. Μόλις η καταγραφή φτάσει στο όριο, μπορεί να γίνει επανενεργοποίηση της με το μηδενισμό του μετρητή καταγραφής, ή του μετρητή για το συγκεκριμένο κανόνα. Δείτε την εντολή `ipfw reset log`.

Η καταγραφή γίνεται μόνο αφού επαληθευθούν όλες οι άλλες συνθήκες ταιριάσματος του πακέτου, και πριν την τελική αποδοχή ή απόρριψη του. Είναι στη

> δική σας ευχέρεια να αποφασίσετε σε ποιους κανόνες θα ενεργοποιήσετε την καταγραφή.

55.6.5.1.5. Επιλογή

Οι λέξεις-κλειδιά που περιγράφονται σε αυτή την ενότητα, χρησιμοποιούνται για να περιγράψουν χαρακτηριστικά του πακέτου που θα πρέπει να διερευνηθούν για να καθοριστεί αν το πακέτο ταιριάζει ή όχι με τον κανόνα. Η επιλογή μπορεί να γίνει με βάση τα παρακάτω γενικής φύσεως χαρακτηριστικά, τα οποία και θα πρέπει να χρησιμοποιηθούν με τη σειρά που φαίνονται:

udp | tcp | icmp

Μπορούν επίσης να χρησιμοποιηθούν τα πρωτόκολλα που περιέχονται στο αρχείο /etc/protocols. Η τιμή που καθορίζεται χρησιμοποιείται για το ταίριασμα του πρωτοκόλλου. Πρόκειται για υποχρεωτική παράμετρο.

from src to dst

Οι λέξεις `from` και `to` χρησιμοποιούνται για το ταίριασμα IP διευθύνσεων. Οι κανόνες πρέπει να καθορίζουν *τόσο* την πηγή όσο και τον προορισμό. Η λέξη `any` μπορεί να χρησιμοποιηθεί για ταίριασμα με οποιαδήποτε διεύθυνση. Η λέξη `me` έχει επίσης ειδική σημασία. Ταιριάζει με οποιαδήποτε διεύθυνση που έχει ρυθμιστεί σε κάποια διεπαφή του συστήματος σας, αντιπροσωπεύοντας έτσι το PC στο οποίο εκτελείται το firewall. Μπορούν έτσι να γραφούν κανόνες του τύπου `from me to any` ή `from any to me` ή `from any to 0.0.0.0/0` ή `from 0.0.0.0/0 to me` ή `from any to 0.0.0.0` ή `from me to 0.0.0.0`. Οι διευθύνσεις IP καθορίζονται ως αριθμητικές οκτάδες χωρισμένες με τελείες και ακολουθούνται από το μήκος της μάσκας υποδικτύου. Μια IP διεύθυνση μπορεί να καθορίζεται με αριθμούς που χωρίζονται με τελείες. Μπορεί επίσης να ακολουθείται από το μέγεθος της μάσκας υποδικτύου (μορφή CIDR). Πρόκειται για υποχρεωτική παράμετρο. Μπορείτε να χρησιμοποιήσετε το βοηθητικό πρόγραμμα net-mgmt/ipcalc για διευκόλυνση σας στους υπολογισμούς. Δείτε την δικτυακή τοποθεσία του προγράμματος για περισσότερες πληροφορίες: http://jodies.de/ipcalc.

port number

Χρησιμοποιείται σε πρωτόκολλα που υποστηρίζουν αριθμούς θυρών (όπως είναι τα TCP και UDP). Είναι υποχρεωτικό να δίνεται ο αριθμός θύρας της υπηρεσίας που θέλετε να ταιριάξετε. Μπορείτε να χρησιμοποιήσετε τα ονόματα των υπηρεσιών (μπορείτε να τα βρείτε στο αρχείο /etc/services) αντί για τους κανονικούς αριθμούς θυρών.

in | out

Με το παραπάνω μπορεί να καθοριστεί αν το ταίριασμα θα γίνεται σε εισερχόμενα ή σε εξερχόμενα πακέτα αντίστοιχα. Είναι υποχρεωτικό να έχετε ως μέρος των κριτηρίων του κανόνα σας, είτε τη λέξη `in` είτε τη λέξη `out`.

via IF

Ταιριάζει τα πακέτα τα οποία διέρχονται μέσω της διεπαφής με το όνομα που καθορίζεται. Η λέξη `via` εξασφαλίζει ότι το όνομα της διεπαφής θα είναι πάντα μέρος των κριτηρίων κατά τη διαδικασία ταιριάσματος.

setup

Πρόκειται για υποχρεωτική παράμετρο που αναγνωρίζει την αίτηση έναρξης μιας συνεδρίας για πακέτα TCP.

keep-state

Πρόκειται για υποχρεωτική παράμετρο. Μόλις υπάρξει ταίριασμα, το firewall θα δημιουργήσει ένα δυναμικό κανόνα, του οποίου η προεπιλεγμένη συμπεριφορά είναι να ταιριάζει επικοινωνία διπλής κατεύθυνσης μεταξύ της διεύθυνσης IP και της θύρας αφετηρίας και προορισμού, χρησιμοποιώντας το ίδιο πρωτόκολλο.

limit {src-addr | src-port | dst-addr | dst-port}

Το firewall θα επιτρέψει μόνο *N* πλήθος συνδέσεων με τις παραμέτρους που περιγράφονται σε αυτό τον κανόνα. Μπορούν να καθοριστούν περισσότερες από μια διευθύνσεις και πόρτες αφετηρίας και προορισμού. Δεν μπορούν να χρησιμοποιηθούν στον ίδιο κανόνα οι παράμετροι `limit` και `keep-state`. Η επιλογή `limit` παρέχει την ίδια λειτουργία stateful με την `keep-state`, καθώς και επιπρόσθετες δικές της λειτουργίες.

55.6.5.2. Επιλογή για Stateful Κανόνες

Το stateful φιλτράρισμα, αντιμετωπίζει την κίνηση του δικτύου ως διπλής κατεύθυνσης ανταλλαγή πακέτων τα οποία δημιουργούν μια συνεδρία. Έχει επίσης τη δυνατότητα να διερευνήσει αν τηρούνται οι έγκυροι κανόνες ανταλλαγής μηνυμάτων μεταξύ του αποστολέα και του παραλήπτη. Οποιαδήποτε πακέτα δεν ταιριάζουν με το πρότυπο αυτής της επικοινωνίας, απορρίπτονται ως ψεύτικα.

Η επιλογή `check-state` χρησιμοποιείται για να αναγνωριστεί σε ποιο σημείο του συνόλου κανόνων του IPFW θα ελεγχθεί το πακέτο με βάση τη δυνατότητα των δυναμικών κανόνων. Σε περίπτωση ταιριάσματος, το πακέτο εξέρχεται από το firewall και συνεχίζει την πορεία του, ενώ την ίδια στιγμή δημιουργείται ένας νέος δυναμικός κανόνας για το επόμενο πακέτο που αναμένεται να έρθει με βάση τη συγκεκριμένη διπλής κατεύθυνσης επικοινωνία. Σε περίπτωση που το πακέτο δεν ταιριάζει με το δυναμικό κανόνα, θα προχωρήσει για να ελεγχθεί από τον επόμενο κανόνα του firewall.

Η δυνατότητα δυναμικών κανόνων είναι ευάλωτη σε εξάντληση πόρων σε περίπτωση επίθεσης υπερχείλισης (flood) SYN. Η επίθεση αυτή μπορεί να δημιουργήσει πολύ μεγάλο πλήθος δυναμικών κανόνων. Για την αντιμετώπιση μιας τέτοιας επίθεσης, το FreeBSD χρησιμοποιεί μια ακόμα επιλογή που ονομάζεται `limit`. Η επιλογή αυτή μπορεί να περιορίσει τον αριθμό των ταυτόχρονων συνεδριών, εξετάζοντας τα πεδία αφετηρίας και προορισμού των κανόνων. Ανιχνεύει με αυτό τον τρόπο το πλήθος των δυναμικών κανόνων και πόσες φορές έχει χρησιμοποιηθεί ο καθένας από τη συγκεκριμένη IP διεύθυνση. Αν ο αριθμός αυτός ξεπερνάει το όριο που έχει τεθεί με την επιλογή `limit`, το πακέτο απορρίπτεται.

55.6.5.3. Καταγραφή Μηνυμάτων του Firewall

Τα πλεονεκτήματα της καταγραφής συμβάντων του firewall, είναι προφανή: παρέχουν τη δυνατότητα να δείτε για ποιο λόγο ενεργοποιήθηκαν οι κανόνες στους οποίους έχετε ενεργοποιήσει την καταγραφή. Οι πληροφορίες περιλαμβάνουν τα πακέτα που απορρίφθηκαν, τις διευθύνσεις από τις οποίες προήλθαν και που κατευθύνονταν. Με αυτό τον τρόπο, έχετε ένα σημαντικό πλεονέκτημα

στην ανίχνευση των εισβολέων.

Ακόμα και αν ενεργοποιήσετε τη λειτουργία καταγραφής, το IPFW δεν θα αρχίσει από μόνο του την καταγραφή για κανένα κανόνα. Ο διαχειριστής του firewall θα αποφασίσει σε ποιους από όλους τους κανόνες θα ενεργοποιήσει την καταγραφή, και θα προσθέσει την λέξη `log` στην αντίστοιχη καταχώριση. Φυσιολογικά, γίνεται καταγραφή μόνο για κανόνες που απορρίπτουν πακέτα (κανόνες `deny`), όπως για παράδειγμα ο κανόνας απόρριψης των εισερχόμενων ICMP pings. Είναι κοινή πρακτική, να αντιγράφεται στο τέλος των κανόνων ο κανόνας "ipfw default deny everything" και να προστίθεται σε αυτόν η επιλογή `log`. Με τον τρόπο αυτό, μπορείτε να δείτε όλα τα πακέτα που δεν ταίριαξαν με κανένα κανόνα του συνόλου.

Η καταγραφή συμβάντων είναι δίκοπο μαχαίρι. Αν δεν είστε προσεκτικός, θα χαθείτε μέσα στο πλήθος των δεδομένων της καταγραφής και θα γεμίσετε το δίσκο σας με άχρηστα αρχεία. Οι πιο παλιές και κοινές επιθέσεις τύπου άρνησης υπηρεσίας (DoS), είναι αυτές που προσπαθούν να γεμίσουν τους δίσκους σας. Τα μηνύματα αυτά όχι μόνο καταγράφονται στο syslogd, αλλά εμφανίζονται και στην κονσόλα του συστήματος σας, και σύντομα γίνονται πολύ ενοχλητικά.

Η επιλογή `IPFIREWALL_VERBOSE_LIMIT=5` στον πυρήνα, περιορίζει τον αριθμό των συνεχόμενων όμοιων μηνυμάτων που στέλνονται στον καταγραφέα συστήματος syslogd(8) σχετικά με το ταίριασμα πακέτων ενός συγκεκριμένου κανόνα. Όταν ενεργοποιείται αυτή η επιλογή στον πυρήνα, ο αριθμός των συνεχόμενων μηνυμάτων ενός συγκεκριμένου κανόνα, σταματάει μετά τον αριθμό που καθορίζεται. Δεν υπάρχει κανένα όφελος από 200 συνεχόμενα μηνύματα με το ίδιο ακριβώς περιεχόμενο. Για παράδειγμα, πέντε συνεχόμενα μηνύματα για ένα συγκεκριμένο κανόνα θα καταγράφονταν κανονικά στο syslogd. Τα υπόλοιπα όμοια μηνύματα θα καταμετρηθούν και θα καταγραφούν όπως φαίνεται παρακάτω:

```
last message repeated 45 times
```

Όλα τα μηνύματα καταγραφής των πακέτων, γράφονται από προεπιλογή στο αρχείο /var/log/security το οποίο καθορίζεται στο αρχείο /etc/syslog.conf.

55.6.5.4. Δημιουργία Ενός Script Κανόνων

Οι περισσότεροι έμπειροι χρήστες του IPFW, δημιουργούν ένα αρχείο που περιέχει τους κανόνες και το γράφουν με τέτοιο τρόπο ώστε να να μπορεί να εκτελεστεί ως script. Το βασικό πλεονέκτημα του παραπάνω τρόπου, είναι ότι οι κανόνες του firewall μπορούν να ανανεωθούν χωρίς την ανάγκη να επανεκκινήσει το σύστημα για να φορτωθούν οι νέοι. Η μέθοδος αυτή είναι πολύ βολική για την δοκιμή νέων κανόνων, καθώς η διαδικασία μπορεί να επαναληφθεί όσες φορές χρειάζεται. Καθώς πρόκειται για κανονικό script, μπορείτε να χρησιμοποιήσετε συμβολική υποκατάσταση για να κωδικοποιήσετε και να υποκαταστήσετε συχνά χρησιμοποιούμενες τιμές σε πολλαπλούς κανόνες. Αυτό φαίνεται στο παρακάτω παράδειγμα.

Η σύνταξη που χρησιμοποιείται εδώ, είναι συμβατή με τα κελύφη sh(1), csh(1) και tcsh(1). Μπροστά από τα πεδία της συμβολικής υποκατάστασης, υπάρχει το σήμα του δολαρίου, $. Το σύμβολο αυτό δεν υπάρχει μπροστά από τα συμβολικά πεδία. Η τιμή που θα αποδοθεί στο συμβολικό πεδίο, πρέπει να εσωκλείεται σε διπλά εισαγωγικά.

Ξεκινήστε το αρχείο των κανόνων σας όπως φαίνεται παρακάτω:

```
############### start of example ipfw rules script #############
#
ipfw -q -f flush       # Delete all rules
# Set defaults
oif="tun0"             # out interface
odns="192.0.2.11"      # ISP's DNS server IP address
cmd="ipfw -q add "     # build rule prefix
ks="keep-state"        # just too lazy to key this each time
$cmd 00500 check-state
$cmd 00502 deny all from any to any frag
$cmd 00501 deny tcp from any to any established
$cmd 00600 allow tcp from any to any 80 out via $oif setup $ks
$cmd 00610 allow tcp from any to $odns 53 out via $oif setup $ks
$cmd 00611 allow udp from any to $odns 53 out via $oif $ks
################### End of example ipfw rules script #############
```

Αυτό είναι όλο. Στο παράδειγμα αυτό δεν είναι σημαντικοί οι κανόνες, αλλά ο τρόπος με τον οποίο λειτουργούν και παίρνουν τιμές τα πεδία συμβολικής υποκατάστασης.

Αν το παραπάνω παράδειγμα ήταν στο αρχείο /etc/ipfw.rules θα μπορούσατε να φορτώσετε αυτούς τους κανόνες, γράφοντας την παρακάτω εντολή:

```
# sh /etc/ipfw.rules
```

Το αρχείο /etc/ipfw.rules μπορεί να βρίσκεται σε όποιο κατάλογο θέλετε, και να ονομάζεται επίσης όπως θέλετε.

Θα μπορούσατε να επιτύχετε το ίδιο πράγμα, εκτελώντας τις παρακάτω εντολές χειροκίνητα:

```
# ipfw -q -f flush
# ipfw -q add check-state
# ipfw -q add deny all from any to any frag
# ipfw -q add deny tcp from any to any established
# ipfw -q add allow tcp from any to any 80 out via tun0 setup keep-state
# ipfw -q add allow tcp from any to 192.0.2.11 53 out via tun0 setup keep-state
# ipfw -q add 00611 allow udp from any to 192.0.2.11 53 out via tun0 keep-state
```

55.6.5.5. Σύνολο Κανόνων Stateful

Το παρακάτω σύνολο κανόνων (που δεν περιέχει κανόνες για NAT) είναι ένα παράδειγμα γραφής ενός inclusive firewall. Ένα inclusive firewall επιτρέπει την είσοδο μόνο των πακέτων που ταιριάζουν με τους κανόνες αποδοχής (pass) και απορρίπτει από προεπιλογή όλα τα άλλα. Τα firewalls που έχουν σχεδιαστεί να προστατεύουν ολόκληρα δίκτυα, διαθέτουν το λιγότερο δύο διεπαφές, στις οποίες πρέπει να υπάρχουν κανόνες ώστε το firewall να λειτουργεί.

Όλα τα λειτουργικά συστήματα τύπου UNIX®, συμπεριλαμβανομένου και του FreeBSD, έχουν σχεδιαστεί να χρησιμοποιούν τη διεπαφή lo0 και τη διεύθυνση IP 127.0.0.1 για εσωτερική

επικοινωνία με το λειτουργικό σύστημα. Το firewall πρέπει να περιέχει κανόνες που να επιτρέπουν την απρόσκοπτη κίνηση αυτών των ειδικών, για εσωτερική χρήση, πακέτων.

Οι κανόνες που ορίζουν την πρόσβαση εισερχόμενων και εξερχόμενων πακέτων, γράφονται για τη διεπαφή που συνδέεται στο δημόσιο Internet. Η διεπαφή αυτή μπορεί να είναι για παράδειγμα η tun0 (σε περίπτωση που χρησιμοποιείτε το PPP χρήστη), ή η κάρτα δικτύου που συνδέεται στο καλωδιακό ή DSL modem σας.

Σε περίπτωση που μια ή περισσότερες κάρτες δικτύου συνδέονται σε εσωτερικά ιδιωτικά δίκτυα πίσω από το firewall, θα πρέπει να υπάρχουν οι αντίστοιχοι κανόνες που να επιτρέπουν την ελεύθερη διακίνηση των πακέτων ανάμεσα στις διεπαφές αυτές ή/και στο Internet.

Οι κανόνες πρέπει να οργανώνονται σε τρεις κύριες ενότητες: αρχικά όλες οι διεπαφές στις οποίες επιτρέπεται η ελεύθερη διακίνηση δεδομένων, έπειτα η διεπαφή από την οποία εξέρχονται τα πακέτα προς το δημόσιο δίκτυο (Internet) και τέλος η διεπαφή από την οποία λαμβάνονται πακέτα από το Internet.

Σε κάθε μια από τις ενότητες των διεπαφών που συνδέονται στο Internet, πρέπει να τοποθετούνται πρώτοι οι κανόνες που ταιριάζουν συχνότερα με την αντίστοιχη κίνηση. Ο τελευταίος κανόνας της ενότητας θα πρέπει να απορρίπτει και να καταγράφει όλα τα πακέτα της συγκεκριμένης διεπαφής/κατεύθυνσης.

Η ενότητα εξερχομένων (Outbound) στο σύνολο κανόνων που φαίνεται παρακάτω, περιέχει μόνο κανόνες τύπου `allow`. Οι κανόνες αυτοί περιέχουν συγκεκριμένες επιλεγμένες τιμές, με τις οποίες αναγνωρίζεται με μοναδικό τρόπο η υπηρεσία στην οποία επιτρέπεται η πρόσβαση από το δημόσιο Internet. Όλοι οι κανόνες έχουν τις επιλογές `proto`, `port`, `in/out` και `keep-state`. Οι κανόνες τύπου `proto tcp` περιέχουν την επιλογή `setup` για την αναγνώριση του πακέτου έναρξης της συνεδρίας, ώστε να γίνει η καταχώριση της στον πίνακα συνδέσεων (stateful).

Στην ενότητα των εισερχόμενων πακέτων (Inbound) που φαίνεται παρακάτω, εμφανίζονται πρώτοι οι κανόνες που χρησιμοποιούνται για την απόρριψη των ανεπιθύμητων πακέτων. Αυτό γίνεται για δύο διαφορετικούς λόγους. Ο πρώτος είναι ότι τα κακόβουλα πακέτα μπορεί εν μέρει να ταιριάζουν με κάποια χαρακτηριστικά της έγκυρης κίνησης. Τα πακέτα αυτά θα πρέπει να απορριφθούν, αντί να γίνουν δεκτά από κάποιο επόμενο κανόνα `allow`. Ο δεύτερος είναι ότι μπορείτε να απορρίψετε συγκεκριμένα πακέτα τα οποία γνωρίζετε ότι δεν είναι έγκυρα, αλλά σας είναι αδιάφορη η καταγραφή τους. Με τον τρόπο αυτό εμποδίζεται η λήψη και καταγραφή τους από τον τελευταίο κανόνα. Ο τελευταίος κανόνας τυπικά απορρίπτει και καταγράφει όλα τα πακέτα που έφτασαν μέχρι αυτόν. Ο κανόνας αυτός χρησιμοποιείται για την παροχή νομικών αποδείξεων σε περίπτωση που κινήσετε νομική διαδικασία κατά ατόμων που προέβησαν σε επιθέσεις στο σύστημα σας.

Θα πρέπει επίσης να εξασφαλίσετε ότι το σύστημα σας δεν θα δώσει καμιά απάντηση σε κανένα από τα ανεπιθύμητα πακέτα. Τα πακέτα αυτά θα πρέπει να απορριφθούν και να εξαφανιστούν. Με τον τρόπο αυτό, ο επιτιθέμενος δεν έχει καμιά γνώση αν τα πακέτα του έφτασαν μέχρι το σύστημα σας. Όσο λιγότερα μπορούν να μάθουν οι επιτιθέμενοι σχετικά με το σύστημα σας, τόσο πιο ασφαλές είναι. Όταν εκτελείτε καταγραφή πακέτων με αριθμούς θυρών που δεν αναγνωρίζετε, κοιτάξτε στο αρχείο /etc/services/ ή δείτε το http://www.securitystats.com/tools/portsearch.php και αναζητήστε τον αριθμό της θύρας για να δείτε ποιος είναι ο σκοπός της. Ελέγξτε την παρακάτω τοποθεσία για τους αριθμούς θυρών που χρησιμοποιούνται συχνά από κακόβουλα προγράμματα (Trojans): http://www.simovits.com/trojans/trojans.html.

55.6.5.6. Ένα Υπόδειγμα Συνόλου Κανόνων Inclusive

Το παρακάτω σύνολο κανόνων (στο οποίο δεν υλοποιείται λειτουργία NAT) είναι αρκετά πλήρες και πολύ ασφαλές. Δημιουργεί firewall τύπου inclusive, και έχει δοκιμαστεί σε πραγματικές συνθήκες λειτουργίας. Μπορεί να εξυπηρετήσει το ίδιο καλά και το δικό σας σύστημα. Απλώς μετατρέψτε σε σχόλιο τους κανόνες `pass` για τις υπηρεσίες που δεν θέλετε να ενεργοποιήσετε. Για να αποφύγετε την καταγραφή ανεπιθύμητων μηνυμάτων, απλώς προσθέστε ένα κανόνα τύπου `deny` στην ενότητα των εισερχομένων. Σε όλους τους κανόνες, Θα πρέπει να αλλάξετε το όνομα της διεπαφής από dc0 στο πραγματικό όνομα της διεπαφής που συνδέεται στο δημόσιο Internet. Σε περίπτωση που χρησιμοποιείτε το PPP χρήστη, το όνομα της διεπαφής θα είναι tun0.

Θα διαπιστώσετε ότι υπάρχει μια συγκεκριμένη λογική στη χρήση αυτών των κανόνων.

- Όλοι οι κανόνες που αποτελούν αίτηση για έναρξη μιας νέας συνεδρίας με το δημόσιο Internet, χρησιμοποιούν την επιλογή `keep-state`.
- Όλες οι διαπιστευμένες υπηρεσίες που προέρχονται από το δημόσιο Internet, διαθέτουν την επιλογή `limit`, για την αποφυγή επιθέσεων υπερχείλισης (flooding).
- Όλοι οι κανόνες χρησιμοποιούν τις επιλογές `in` ή `out` για να διευκρινίζουν την κατεύθυνση της επικοινωνίας.
- Όλοι οι κανόνες χρησιμοποιούν την επιλογή `via όνομα-διεπαφής` για να καθορίσουν τη διεπαφή από την οποία διέρχεται το πακέτο.

Οι κανόνες που φαίνονται παρακάτω, θα πρέπει να γραφούν στο /etc/ipfw.rules.

```
################ Start of IPFW rules file ###################################
# Flush out the list before we begin.
ipfw -q -f flush

# Set rules command prefix
cmd="ipfw -q add"
pif="dc0"     # public interface name of NIC
              # facing the public Internet

#####################################################################
# No restrictions on Inside LAN Interface for private network
# Not needed unless you have LAN.
# Change xl0 to your LAN NIC interface name
#####################################################################
#$cmd 00005 allow all from any to any via xl0

#####################################################################
# No restrictions on Loopback Interface
#####################################################################
$cmd 00010 allow all from any to any via lo0

#####################################################################
# Allow the packet through if it has previous been added to the
# the "dynamic" rules table by a allow keep-state statement.
#####################################################################
```

```
$cmd 00015 check-state

#####################################################################
# Interface facing Public Internet (Outbound Section)
# Check session start requests originating from behind the
# firewall on the private network or from this gateway server
# destined for the public Internet.
#####################################################################

# Allow out access to my ISP's Domain name server.
# x.x.x.x must be the IP address of your ISP.s DNS
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
$cmd 00110 allow tcp from any to x.x.x.x 53 out via $pif setup keep-state
$cmd 00111 allow udp from any to x.x.x.x 53 out via $pif keep-state

# Allow out access to my ISP's DHCP server for cable/DSL configurations.
# This rule is not needed for .user ppp. connection to the public Internet.
# so you can delete this whole group.
# Use the following rule and check log for IP address.
# Then put IP address in commented out rule & delete first rule
$cmd 00120 allow log udp from any to any 67 out via $pif keep-state
#$cmd 00120 allow udp from any to x.x.x.x 67 out via $pif keep-state

# Allow out non-secure standard www function
$cmd 00200 allow tcp from any to any 80 out via $pif setup keep-state

# Allow out secure www function https over TLS SSL
$cmd 00220 allow tcp from any to any 443 out via $pif setup keep-state

# Allow out send & get email function
$cmd 00230 allow tcp from any to any 25 out via $pif setup keep-state
$cmd 00231 allow tcp from any to any 110 out via $pif setup keep-state

# Allow out FBSD (make install & CVSUP) functions
# Basically give user root "GOD" privileges.
$cmd 00240 allow tcp from me to any out via $pif setup keep-state uid root

# Allow out ping
$cmd 00250 allow icmp from any to any out via $pif keep-state

# Allow out Time
$cmd 00260 allow tcp from any to any 37 out via $pif setup keep-state

# Allow out nntp news (i.e. news groups)
$cmd 00270 allow tcp from any to any 119 out via $pif setup keep-state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
$cmd 00280 allow tcp from any to any 22 out via $pif setup keep-state
```

```
# Allow out whois
$cmd 00290 allow tcp from any to any 43 out via $pif setup keep-state

# deny and log everything else that.s trying to get out.
# This rule enforces the block all by default logic.
$cmd 00299 deny log all from any to any out via $pif

#####################################################################
# Interface facing Public Internet (Inbound Section)
# Check packets originating from the public Internet
# destined for this gateway server or the private network.
#####################################################################

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 00300 deny all from 192.168.0.0/16 to any in via $pif  #RFC 1918 private IP
$cmd 00301 deny all from 172.16.0.0/12 to any in via $pif     #RFC 1918 private IP
$cmd 00302 deny all from 10.0.0.0/8 to any in via $pif          #RFC 1918 private IP
$cmd 00303 deny all from 127.0.0.0/8 to any in via $pif        #loopback
$cmd 00304 deny all from 0.0.0.0/8 to any in via $pif            #loopback
$cmd 00305 deny all from 169.254.0.0/16 to any in via $pif   #DHCP auto-config
$cmd 00306 deny all from 192.0.2.0/24 to any in via $pif       #reserved for docs
$cmd 00307 deny all from 204.152.64.0/23 to any in via $pif  #Sun cluster interconnect
$cmd 00308 deny all from 224.0.0.0/3 to any in via $pif         #Class D & E multicast

# Deny public pings
$cmd 00310 deny icmp from any to any in via $pif

# Deny ident
$cmd 00315 deny tcp from any to any 113 in via $pif

# Deny all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
$cmd 00320 deny tcp from any to any 137 in via $pif
$cmd 00321 deny tcp from any to any 138 in via $pif
$cmd 00322 deny tcp from any to any 139 in via $pif
$cmd 00323 deny tcp from any to any 81 in via $pif

# Deny any late arriving packets
$cmd 00330 deny all from any to any frag in via $pif

# Deny ACK packets that did not match the dynamic rule table
$cmd 00332 deny tcp from any to any established in via $pif

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP.s DHCP server as it.s the only
# authorized source to send this packet type.
# Only necessary for cable or DSL configurations.
# This rule is not needed for .user ppp. type connection to
# the public Internet. This is the same IP address you captured
# and used in the outbound section.
```

```
#$cmd 00360 allow udp from any to x.x.x.x 67 in via $pif keep-state

# Allow in standard www function because I have apache server
$cmd 00400 allow tcp from any to me 80 in via $pif setup limit src-addr 2

# Allow in secure FTP, Telnet, and SCP from public Internet
$cmd 00410 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID & PW are passed over public
# Internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
$cmd 00420 allow tcp from any to me 23 in via $pif setup limit src-addr 2

# Reject & Log all incoming connections from the outside
$cmd 00499 deny log all from any to any in via $pif

# Everything else is denied by default
# deny and log all packets that fell through to see what they are
$cmd 00999 deny log all from any to any
################## End of IPFW rules file ###################################
```

55.6.5.7. Ένα Υπόδειγμα NAT με Stateful Σύνολο Κανόνων

Για να ενεργοποιηθεί η λειτουργία NAT στο IPFW, χρειάζονται κάποιες επιπλέον ρυθμίσεις. Θα πρέπει να προσθέσετε την επιλογή `option IPDIVERT` μαζί με τις υπόλοιπες επιλογές για το IPFIREWALL στο αρχείο ρυθμίσεων του πυρήνα. Θα πρέπει έπειτα να μεταγλωττίσετε και να εγκαταστήσετε το νέο σας προσαρμοσμένο πυρήνα.

Εκτός από τις συνηθισμένες επιλογές για το IPFW, θα πρέπει να προσθέσετε και τις παρακάτω στο αρχείο /etc/rc.conf:

```
natd_enable="YES"                   # Enable NATD function
natd_interface="rl0"                # interface name of public Internet NIC
natd_flags="-dynamic -m"            # -m = preserve port numbers if possible
```

Η χρήση κανόνων stateful μαζί με τον κανόνα `divert natd` (NAT), περιπλέκει πολύ την λογική συγγραφής των κανόνων. Η θέση εμφάνισης των κανόνων `check-state` και `divert natd` μέσα στο σύνολο κανόνων γίνεται πολύ κρίσιμη. Δεν πρόκειται πλέον για απλή λογική περάσματος από τον ένα κανόνα στον επόμενο. Χρησιμοποιείται ένα νέο είδος ενέργειας που ονομάζεται `skipto`. Για να χρησιμοποιηθεί η εντολή `skipto`, είναι υποχρεωτικό να έχετε αριθμήσει τους κανόνες, ώστε να ξέρετε σε ποιο κανόνα θα καταλήξει το άλμα που θα εκτελεστεί από την εντολή αυτή.

Παρακάτω θα βρείτε ένα υπόδειγμα (χωρίς πρόσθετα σχόλια) μιας μεθόδου συγγραφής που επιλέξαμε εδώ για να εξηγήσουμε την ακολουθία ροής του πακέτου μέσα στο σύνολο κανόνων.

Η ροή της επεξεργασίας ξεκινάει με τον πρώτο από την κορυφή κανόνα και συνεχίζει ένα κανόνα κάθε φορά προς τα κάτω, είτε μέχρι να φτάσει τον τελευταίο, ή μέχρι το πακέτο να ταιριάξει με τα κριτήρια επιλογής κάποιου κανόνα και να ελευθερωθεί από το firewall. Είναι σημαντικό να

παρατηρήσουμε τη θέση των κανόνων με αριθμούς 100, 101, 450, 500 και 510. Οι κανόνες αυτοί ελέγχουν την μετάφραση των εξερχόμενων και εισερχόμενων πακέτων, ώστε οι καταχωρήσεις τους στο δυναμικό πίνακα καταστάσεων να περιέχουν πάντα την ιδιωτική IP διεύθυνση του τοπικού δικτύου. Παρατηρήστε επίσης ότι όλοι οι κανόνες allow και deny καθορίζουν την κατεύθυνση κίνησης του πακέτου καθώς και την διεπαφή. Επίσης, όλες οι εξερχόμενες αιτήσεις για νέες συνεδρίες μεταφέρονται απευθείας (μέσω του `skipto rule 500`) στον κανόνα 500 για να γίνει η μετάφραση διευθύνσεων δικτύου (NAT).

Ας υποθέσουμε ότι ένα χρήστης του τοπικού δικτύου χρησιμοποιεί τον φυλλομετρητή του για να δει μια ιστοσελίδα. Οι ιστοσελίδες χρησιμοποιούν την πόρτα 80 για την επικοινωνία. Το πακέτο εισέρχεται στο firewall. Δεν ταιριάζει με τον κανόνα 100 γιατί είναι εξερχόμενο και όχι εισερχόμενο. Περνάει τον κανόνα 101 γιατί πρόκειται για νέα επικοινωνία και έτσι δεν υπάρχει ακόμα στον δυναμικό πίνακα καταστάσεων. Το πακέτο τελικά φτάνει στον κανόνα 125 με τον οποίο και ταιριάζει. Εξέρχεται μέσω της κάρτας δικτύου που συνδέεται στο δημόσιο Internet. Το πακέτο έχει ακόμα ως IP αφετηρίας την ιδιωτική διεύθυνση του τοπικού δικτύου. Το ταίριασμα με αυτό τον κανόνα προκαλεί δύο ενέργειες. Η επιλογή `keep-state` θα δημιουργήσει ένα νέο δυναμικό κανόνα, θα τον καταχωρήσει στον πίνακα, και θα εκτελέσει την αντίστοιχη ενέργεια. Η ενέργεια αυτή είναι μέρος της πληροφορίας που γράφεται στον δυναμικό πίνακα. Στην περίπτωση αυτή είναι η "skipto rule 500". Ο κανόνας 500 μεταφράζει μέσω NAT τη διεύθυνση IP του πακέτου, πριν αυτό εξέλθει προς το Internet. Αυτό είναι ιδιαίτερα σημαντικό. Το πακέτο κατευθύνεται προς τον προορισμό του, όπου δημιουργείται και αποστέλλεται ένα νέο πακέτο ως απάντηση. Το νέο αυτό πακέτο εισέρχεται ξανά στο firewall, στον κανόνα που είναι στην κορυφή της λίστας. Αυτή τη φορά ταιριάζει με τον κανόνα 100 και η διεύθυνση προορισμού του αλλάζει ξανά στην αρχική του τοπικού δικτύου. Έπειτα, γίνεται η επεξεργασία του από τον κανόνα `check-state` ο οποίος ανακαλύπτει ότι πρόκειται για πακέτο συνεδρίας σε εξέλιξη και το απελευθερώνει στο τοπικό δίκτυο. Κατευθύνεται προς τον υπολογιστή του τοπικού δικτύου που το έστειλε, ο οποίος στέλνει ένα νέο πακέτο ζητώντας περισσότερα δεδομένα από τον απομακρυσμένο εξυπηρετητή. Το πακέτο αυτό ελέγχεται από τον κανόνα `check-state`, ο οποίος βρίσκει την καταχώριση του στα εξερχόμενα και εκτελεί την αντίστοιχη ενέργεια που σε αυτή την περίπτωση είναι "skipto 500". Το πακέτο προωθείται στον κανόνα 500, γίνεται η μετάφραση της διεύθυνσης του μέσω NAT και απελευθερώνεται στο Internet.

Από την μεριά των εισερχόμενων, όποιο πακέτο αναγνωρίζεται ως μέρος μιας υπάρχουσας συνεδρίας, ελέγχεται αυτόματα από τον κανόνα `check-state` και τους αντίστοιχους κανόνες `divert natd`. Το μόνο που χρειάζεται να αντιμετωπίσουμε είναι η απόρριψη όλων των προβληματικών πακέτων και η έγκριση μόνο των πακέτων που προορίζονται για εγκεκριμένες υπηρεσίες. Ας υποθέσουμε ότι έχουμε ένα εξυπηρετητή apache ο οποίος εκτελείται στο μηχάνημα με το firewall, και επιθυμούμε το τοπικό site να είναι προσβάσιμο από το δημόσιο Internet. Η εισερχόμενη αίτηση νέας συνεδρίας ταιριάζει με τον κανόνα 100 και η IP διεύθυνση της αντιστοιχίζεται στο τοπικό IP του μηχανήματος με το firewall. Το πακέτο έπειτα ελέγχεται για οποιοδήποτε πρόβλημα μπορεί να έχει σύμφωνα με τους κανόνες που χρησιμοποιούμε, και τελικά ταιριάζει με τον κανόνα 425. Στην περίπτωση αυτή συμβαίνουν δύο πράγματα. Ο κανόνας για το πακέτο γράφεται στο δυναμικό πίνακα καταστάσεων, αλλά αυτή τη φορά περιορίζεται ο αριθμός αιτήσεων νέας συνεδρίας από το συγκεκριμένο IP σε 2. Με αυτό τον τρόπο μπορούμε να αμυνθούμε σε επιθέσεις τύπου άρνησης υπηρεσίας (DoS) όσο αφορά τη συγκεκριμένη θύρα επικοινωνίας. Η ενέργεια του κανόνα είναι το `allow`, και έτσι το πακέτο απελευθερώνεται στο τοπικό δίκτυο. Το πακέτο που παράγεται ως απάντηση, ελέγχεται από τον κανόνα `check-state`, ο οποίος αναγνωρίζει ότι ανήκει σε μια ήδη ενεργή συνεδρία, και αποστέλλεται στον κανόνα 500 όπου γίνεται η μετάφραση της διεύθυνσης του μέσω NAT. Το πακέτο τελικά απελευθερώνεται μέσω της διεπαφής εξερχομένων.

Υπόδειγμα Κανόνων #1:

```
#!/bin/sh
cmd="ipfw -q add"
skip="skipto 500"
pif=rl0
ks="keep-state"
good_tcpo="22,25,37,43,53,80,443,110,119"

ipfw -q -f flush

$cmd 002 allow all from any to any via xl0  # exclude LAN traffic
$cmd 003 allow all from any to any via lo0  # exclude loopback traffic

$cmd 100 divert natd ip from any to any in via $pif
$cmd 101 check-state

# Authorized outbound packets
$cmd 120 $skip udp from any to xx.168.240.2 53 out via $pif $ks
$cmd 121 $skip udp from any to xx.168.240.5 53 out via $pif $ks
$cmd 125 $skip tcp from any to any $good_tcpo out via $pif setup $ks
$cmd 130 $skip icmp from any to any out via $pif $ks
$cmd 135 $skip udp from any to any 123 out via $pif $ks

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16  to any in via $pif  #RFC 1918 private IP
$cmd 301 deny all from 172.16.0.0/12   to any in via $pif  #RFC 1918 private IP
$cmd 302 deny all from 10.0.0.0/8      to any in via $pif  #RFC 1918 private IP
$cmd 303 deny all from 127.0.0.0/8     to any in via $pif  #loopback
$cmd 304 deny all from 0.0.0.0/8       to any in via $pif  #loopback
$cmd 305 deny all from 169.254.0.0/16  to any in via $pif  #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24    to any in via $pif  #reserved for docs
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif  #Sun cluster
$cmd 308 deny all from 224.0.0.0/3     to any in via $pif  #Class D & E multicast

# Authorized inbound packets
$cmd 400 allow udp from xx.70.207.54 to any 68 in $ks
$cmd 420 allow tcp from any to me 80 in via $pif setup limit src-addr 1

$cmd 450 deny log ip from any to any

# This is skipto location for outbound stateful rules
$cmd 500 divert natd ip from any to any out via $pif
$cmd 510 allow ip from any to any

######################### end of rules  ##################
```

Οι παρακάτω κανόνες είναι σχεδόν ίδιοι με τους παραπάνω, αλλά περιέχουν περισσότερα σχόλια για να βοηθήσουν τον αρχάριο χρήστη του IPFW να καταλάβει καλύτερα πως λειτουργούν.

Υπόδειγμα Κανόνων #2:

```
#!/bin/sh
################ Start of IPFW rules file ######################################
# Flush out the list before we begin.
ipfw -q -f flush

# Set rules command prefix
cmd="ipfw -q add"
skip="skipto 800"
pif="rl0"     # public interface name of NIC
              # facing the public Internet

#########################################################################
# No restrictions on Inside LAN Interface for private network
# Change xl0 to your LAN NIC interface name
#########################################################################
$cmd 005 allow all from any to any via xl0

#########################################################################
# No restrictions on Loopback Interface
#########################################################################
$cmd 010 allow all from any to any via lo0

#########################################################################
# check if packet is inbound and nat address if it is
#########################################################################
$cmd 014 divert natd ip from any to any in via $pif

#########################################################################
# Allow the packet through if it has previous been added to the
# the "dynamic" rules table by a allow keep-state statement.
#########################################################################
$cmd 015 check-state

#########################################################################
# Interface facing Public Internet (Outbound Section)
# Check session start requests originating from behind the
# firewall on the private network or from this gateway server
# destined for the public Internet.
#########################################################################

# Allow out access to my ISP's Domain name server.
# x.x.x.x must be the IP address of your ISP's DNS
# Dup these lines if your ISP has more than one DNS server
# Get the IP addresses from /etc/resolv.conf file
$cmd 020 $skip tcp from any to x.x.x.x 53 out via $pif setup keep-state

# Allow out access to my ISP's DHCP server for cable/DSL configurations.
$cmd 030 $skip udp from any to x.x.x.x 67 out via $pif keep-state
```

```
# Allow out non-secure standard www function
$cmd 040 $skip tcp from any to any 80 out via $pif setup keep-state

# Allow out secure www function https over TLS SSL
$cmd 050 $skip tcp from any to any 443 out via $pif setup keep-state

# Allow out send & get email function
$cmd 060 $skip tcp from any to any 25 out via $pif setup keep-state
$cmd 061 $skip tcp from any to any 110 out via $pif setup keep-state

# Allow out FreeBSD (make install & CVSUP) functions
# Basically give user root "GOD" privileges.
$cmd 070 $skip tcp from me to any out via $pif setup keep-state uid root

# Allow out ping
$cmd 080 $skip icmp from any to any out via $pif keep-state

# Allow out Time
$cmd 090 $skip tcp from any to any 37 out via $pif setup keep-state

# Allow out nntp news (i.e. news groups)
$cmd 100 $skip tcp from any to any 119 out via $pif setup keep-state

# Allow out secure FTP, Telnet, and SCP
# This function is using SSH (secure shell)
$cmd 110 $skip tcp from any to any 22 out via $pif setup keep-state

# Allow out whois
$cmd 120 $skip tcp from any to any 43 out via $pif setup keep-state

# Allow ntp time server
$cmd 130 $skip udp from any to any 123 out via $pif keep-state

################################################################
# Interface facing Public Internet (Inbound Section)
# Check packets originating from the public Internet
# destined for this gateway server or the private network.
################################################################

# Deny all inbound traffic from non-routable reserved address spaces
$cmd 300 deny all from 192.168.0.0/16  to any in via $pif  #RFC 1918 private IP
$cmd 301 deny all from 172.16.0.0/12   to any in via $pif  #RFC 1918 private IP
$cmd 302 deny all from 10.0.0.0/8      to any in via $pif  #RFC 1918 private IP
$cmd 303 deny all from 127.0.0.0/8     to any in via $pif  #loopback
$cmd 304 deny all from 0.0.0.0/8       to any in via $pif  #loopback
$cmd 305 deny all from 169.254.0.0/16  to any in via $pif  #DHCP auto-config
$cmd 306 deny all from 192.0.2.0/24    to any in via $pif  #reserved for docs
$cmd 307 deny all from 204.152.64.0/23 to any in via $pif  #Sun cluster
$cmd 308 deny all from 224.0.0.0/3     to any in via $pif  #Class D & E multicast
```

```
# Deny ident
$cmd 315 deny tcp from any to any 113 in via $pif

# Deny all Netbios service. 137=name, 138=datagram, 139=session
# Netbios is MS/Windows sharing services.
# Block MS/Windows hosts2 name server requests 81
$cmd 320 deny tcp from any to any 137 in via $pif
$cmd 321 deny tcp from any to any 138 in via $pif
$cmd 322 deny tcp from any to any 139 in via $pif
$cmd 323 deny tcp from any to any 81  in via $pif

# Deny any late arriving packets
$cmd 330 deny all from any to any frag in via $pif

# Deny ACK packets that did not match the dynamic rule table
$cmd 332 deny tcp from any to any established in via $pif

# Allow traffic in from ISP's DHCP server. This rule must contain
# the IP address of your ISP's DHCP server as it's the only
# authorized source to send this packet type.
# Only necessary for cable or DSL configurations.
# This rule is not needed for 'user ppp' type connection to
# the public Internet. This is the same IP address you captured
# and used in the outbound section.
$cmd 360 allow udp from x.x.x.x to any 68 in via $pif keep-state

# Allow in standard www function because I have Apache server
$cmd 370 allow tcp from any to me 80 in via $pif setup limit src-addr 2

# Allow in secure FTP, Telnet, and SCP from public Internet
$cmd 380 allow tcp from any to me 22 in via $pif setup limit src-addr 2

# Allow in non-secure Telnet session from public Internet
# labeled non-secure because ID & PW are passed over public
# Internet as clear text.
# Delete this sample group if you do not have telnet server enabled.
$cmd 390 allow tcp from any to me 23 in via $pif setup limit src-addr 2

# Reject & Log all unauthorized incoming connections from the public Internet
$cmd 400 deny log all from any to any in via $pif

# Reject & Log all unauthorized out going connections to the public Internet
$cmd 450 deny log all from any to any out via $pif

# This is skipto location for outbound stateful rules
$cmd 800 divert natd ip from any to any out via $pif
$cmd 801 allow ip from any to any

# Everything else is denied by default
# deny and log all packets that fell through to see what they are
$cmd 999 deny log all from any to any
```

```
################ End of IPFW rules file ###############################
```

Chapter 56. Προχωρημένα Θέματα Δικτύωσης

56.1. Σύνοψη

Το κεφάλαιο αυτό καλύπτει προχωρημένα θέματα δικτύωσης.

Αφού διαβάσετε αυτό το κεφάλαιο, θα ξέρετε:

- Τα βασικά των πυλών (gateways) και των δρομολογήσεων (routes).
- Πως να ρυθμίσετε συσκευές IEEE 802.11 και Bluetooth®.
- Πως να κάνετε το FreeBSD να δρα ως γέφυρα (bridge).
- Πως να ρυθμίσετε εκκίνηση από το δίκτυο σε ένα μηχάνημα χωρίς σκληρό δίσκο.
- Πως να ρυθμίσετε μετάφραση δικτυακών διευθύνσεων (NAT).
- Πως να συνδέσετε δύο υπολογιστές μέσω PLIP.
- Πως να ρυθμίσετε το IPv6 σε ένα μηχάνημα FreeBSD.
- Πως να ρυθμίσετε το ATM.
- Πως να ρυθμίσετε και να χρησιμοποιήσετε τις δυνατότητες του CARP (Common Access Redundancy Protocol) στο FreeBSD.

Πριν διαβάσετε αυτό το κεφάλαιο, θα πρέπει:

- Να κατανοείτε τις βασικές έννοιες των αρχείων script /etc/rc.
- Να είστε εξοικειωμένος με τη βασική ορολογία των δικτύων.
- Να γνωρίζετε πως να ρυθμίσετε και να εγκαταστήσετε ένα νέο πυρήνα στο FreeBSD (Ρυθμίζοντας τον Πυρήνα του FreeBSD).
- Να γνωρίζετε πως να εγκαταστήσετε πρόσθετο λογισμικό τρίτου κατασκευαστή (Εγκατάσταση Εφαρμογών: Πακέτα και Ports).

56.2. Gateways and Routes

For one machine to be able to find another over a network, there must be a mechanism in place to describe how to get from one to the other. This is called *routing*. A "route" is a defined pair of addresses: a "destination" and a "gateway". The pair indicates that if you are trying to get to this *destination*, communicate through this *gateway*. There are three types of destinations: individual hosts, subnets, and "default". The "default route" is used if none of the other routes apply. We will talk a little bit more about default routes later on. There are also three types of gateways: individual hosts, interfaces (also called "links"), and Ethernet hardware addresses (MAC addresses).

56.2.1. An Example

To illustrate different aspects of routing, we will use the following example from `netstat`:

```
% netstat -r
Routing tables

Destination      Gateway            Flags     Refs     Use     Netif Expire

default          outside-gw         UGSc       37      418      ppp0
localhost        localhost          UH          0      181       lo0
test0            0:e0:b5:36:cf:4f   UHLW        5    63288       ed0     77
10.20.30.255     link#1             UHLW        1     2421
example.com      link#1             UC          0        0
host1            0:e0:a8:37:8:1e    UHLW        3     4601       lo0
host2            0:e0:a8:37:8:1e    UHLW        0        5       lo0 =>
host2.example.com link#1             UC          0        0
224              link#1             UC          0        0
```

The first two lines specify the default route (which we will cover in the next section) and the `localhost` route.

The interface (`Netif` column) that this routing table specifies to use for `localhost` is lo0, also known as the loopback device. This says to keep all traffic for this destination internal, rather than sending it out over the LAN, since it will only end up back where it started.

The next thing that stands out are the addresses beginning with `0:e0:`. These are Ethernet hardware addresses, which are also known as MAC addresses. FreeBSD will automatically identify any hosts (`test0` in the example) on the local Ethernet and add a route for that host, directly to it over the Ethernet interface, ed0. There is also a timeout (`Expire` column) associated with this type of route, which is used if we fail to hear from the host in a specific amount of time. When this happens, the route to this host will be automatically deleted. These hosts are identified using a mechanism known as RIP (Routing Information Protocol), which figures out routes to local hosts based upon a shortest path determination.

FreeBSD will also add subnet routes for the local subnet (`10.20.30.255` is the broadcast address for the subnet `10.20.30`, and `example.com` is the domain name associated with that subnet). The designation `link#1` refers to the first Ethernet card in the machine. You will notice no additional interface is specified for those.

Both of these groups (local network hosts and local subnets) have their routes automatically configured by a daemon called routed. If this is not run, then only routes which are statically defined (i.e. entered explicitly) will exist.

The `host1` line refers to our host, which it knows by Ethernet address. Since we are the sending host, FreeBSD knows to use the loopback interface (lo0) rather than sending it out over the Ethernet interface.

The two `host2` lines are an example of what happens when we use an ifconfig(8) alias (see the section on Ethernet for reasons why we would do this). The ⇒ symbol after the lo0 interface says that not only are we using the loopback (since this address also refers to the local host), but specifically it is an alias. Such routes only show up on the host that supports the alias; all other hosts on the local network will simply have a `link#1` line for such routes.

The final line (destination subnet `224`) deals with multicasting, which will be covered in another section.

Finally, various attributes of each route can be seen in the `Flags` column. Below is a short table of some of these flags and their meanings:

U	Up: The route is active.
H	Host: The route destination is a single host.
G	Gateway: Send anything for this destination on to this remote system, which will figure out from there where to send it.
S	Static: This route was configured manually, not automatically generated by the system.
C	Clone: Generates a new route based upon this route for machines we connect to. This type of route is normally used for local networks.
W	WasCloned: Indicated a route that was auto-configured based upon a local area network (Clone) route.
L	Link: Route involves references to Ethernet hardware.

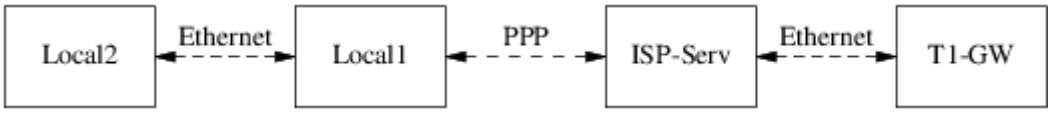
56.2.2. Default Routes

When the local system needs to make a connection to a remote host, it checks the routing table to determine if a known path exists. If the remote host falls into a subnet that we know how to reach (Cloned routes), then the system checks to see if it can connect along that interface.

If all known paths fail, the system has one last option: the "default" route. This route is a special type of gateway route (usually the only one present in the system), and is always marked with a `c` in the flags field. For hosts on a local area network, this gateway is set to whatever machine has a direct connection to the outside world (whether via PPP link, DSL, cable modem, T1, or another network interface).

If you are configuring the default route for a machine which itself is functioning as the gateway to the outside world, then the default route will be the gateway machine at your Internet Service Provider's (ISP) site.

Let us look at an example of default routes. This is a common configuration:



The hosts `Local1` and `Local2` are at your site. `Local1` is connected to an ISP via a dial up PPP connection. This PPP server computer is connected through a local area network to another gateway computer through an external interface to the ISPs Internet feed.

The default routes for each of your machines will be:

Host	Default Gateway	Interface
Local2	Local1	Ethernet
Local1	T1-GW	PPP

A common question is "Why (or how) would we set the `T1-GW` to be the default gateway for `Local1`, rather than the ISP server it is connected to?".

Remember, since the PPP interface is using an address on the ISP's local network for your side of the connection, routes for any other machines on the ISP's local network will be automatically generated. Hence, you will already know how to reach the `T1-GW` machine, so there is no need for the intermediate step of sending traffic to the ISP server.

It is common to use the address `X.X.X.1` as the gateway address for your local network. So (using the same example), if your local class-C address space was `10.20.30` and your ISP was using `10.9.9` then the default routes would be:

Host	Default Route
Local2 (10.20.30.2)	Local1 (10.20.30.1)
Local1 (10.20.30.1, 10.9.9.30)	T1-GW (10.9.9.1)

You can easily define the default route via the /etc/rc.conf file. In our example, on the `Local2` machine, we added the following line in /etc/rc.conf:

```
defaultrouter="10.20.30.1"
```

It is also possible to do it directly from the command line with the route(8) command:

```
# route add default 10.20.30.1
```

For more information on manual manipulation of network routing tables, consult route(8) manual page.

56.2.3. Dual Homed Hosts

There is one other type of configuration that we should cover, and that is a host that sits on two different networks. Technically, any machine functioning as a gateway (in the example above, using a PPP connection) counts as a dual-homed host. But the term is really only used to refer to a machine that sits on two local-area networks.

In one case, the machine has two Ethernet cards, each having an address on the separate subnets. Alternately, the machine may only have one Ethernet card, and be using ifconfig(8) aliasing. The former is used if two physically separate Ethernet networks are in use, the latter if there is one physical network segment, but two logically separate subnets.

Either way, routing tables are set up so that each subnet knows that this machine is the defined gateway (inbound route) to the other subnet. This configuration, with the machine acting as a router between the two subnets, is often used when we need to implement packet filtering or firewall security in either or both directions.

If you want this machine to actually forward packets between the two interfaces, you need to tell FreeBSD to enable this ability. See the next section for more details on how to do this.

56.2.4. Building a Router

A network router is simply a system that forwards packets from one interface to another. Internet standards and good engineering practice prevent the FreeBSD Project from enabling this by default in FreeBSD. You can enable this feature by changing the following variable to `YES` in rc.conf(5):

```
gateway_enable=YES          # Set to YES if this host will be a gateway
```

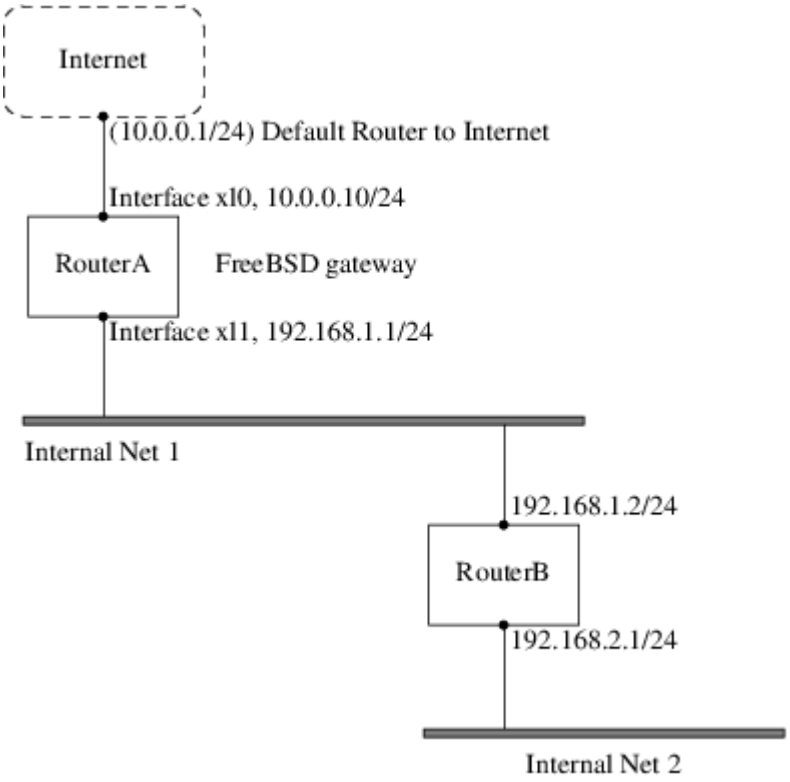
This option will set the sysctl(8) variable `net.inet.ip.forwarding` to `1`. If you should need to stop routing temporarily, you can reset this to `0` temporarily.

Your new router will need routes to know where to send the traffic. If your network is simple enough you can use static routes. FreeBSD also comes with the standard BSD routing daemon routed(8), which speaks RIP (both version 1 and version 2) and IRDP. Support for BGP v4, OSPF v2, and other sophisticated routing protocols is available with the net/zebra package. Commercial products such as GateD® are also available for more complex network routing solutions.

56.2.5. Setting Up Static Routes

56.2.5.1. Manual Configuration

Let us assume we have a network as follows:



In this scenario, `RouterA` is our FreeBSD machine that is acting as a router to the rest of the Internet. It has a default route set to `10.0.0.1` which allows it to connect with the outside world. We will assume that `RouterB` is already configured properly and knows how to get wherever it needs to go. (This is simple in this picture. Just add a default route on `RouterB` using `192.168.1.1` as the gateway.)

If we look at the routing table for `RouterA` we would see something like the following:

```
% netstat -nr
Routing tables

Internet:
Destination        Gateway            Flags    Refs      Use  Netif  Expire
default            10.0.0.1           UGS         0    49378    xl0
127.0.0.1          127.0.0.1          UH          0        6    lo0
10.0.0/24          link#1             UC          0        0    xl0
192.168.1/24       link#2             UC          0        0    xl1
```

With the current routing table `RouterA` will not be able to reach our Internal Net 2. It does not have a route for `192.168.2.0/24`. One way to alleviate this is to manually add the route. The following command would add the Internal Net 2 network to `RouterA`'s routing table using `192.168.1.2` as the next hop:

```
# route add -net 192.168.2.0/24 192.168.1.2
```

Now `RouterA` can reach any hosts on the `192.168.2.0/24` network.

56.2.5.2. Persistent Configuration

The above example is perfect for configuring a static route on a running system. However, one problem is that the routing information will not persist if you reboot your FreeBSD machine. The way to handle the addition of a static route is to put it in your /etc/rc.conf file:

```
# Add Internal Net 2 as a static route
static_routes="internalnet2"
route_internalnet2="-net 192.168.2.0/24 192.168.1.2"
```

The `static_routes` configuration variable is a list of strings separated by a space. Each string references to a route name. In our above example we only have one string in `static_routes`. This string is *internalnet2*. We then add a configuration variable called `route_internalnet2` where we put all of the configuration parameters we would give to the route(8) command. For our example above we would have used the command:

```
# route add -net 192.168.2.0/24 192.168.1.2
```

so we need `"-net 192.168.2.0/24 192.168.1.2"`.

As said above, we can have more than one string in `static_routes`. This allows us to create multiple static routes. The following lines shows an example of adding static routes for the `192.168.0.0/24` and `192.168.1.0/24` networks on an imaginary router:

```
static_routes="net1 net2"
route_net1="-net 192.168.0.0/24 192.168.0.1"
route_net2="-net 192.168.1.0/24 192.168.1.1"
```

56.2.6. Routing Propagation

We have already talked about how we define our routes to the outside world, but not about how the outside world finds us.

We already know that routing tables can be set up so that all traffic for a particular address space (in our examples, a class-C subnet) can be sent to a particular host on that network, which will forward the packets inbound.

When you get an address space assigned to your site, your service provider will set up their routing tables so that all traffic for your subnet will be sent down your PPP link to your site. But how do sites across the country know to send to your ISP?

There is a system (much like the distributed DNS information) that keeps track of all assigned address-spaces, and defines their point of connection to the Internet Backbone. The "Backbone" are the main trunk lines that carry Internet traffic across the country, and around the world. Each backbone machine has a copy of a master set of tables, which direct traffic for a particular network to a specific backbone carrier, and from there down the chain of service providers until it reaches your network.

It is the task of your service provider to advertise to the backbone sites that they are the point of connection (and thus the path inward) for your site. This is known as route propagation.

56.2.7. Troubleshooting

Sometimes, there is a problem with routing propagation, and some sites are unable to connect to you. Perhaps the most useful command for trying to figure out where routing is breaking down is the traceroute(8) command. It is equally useful if you cannot seem to make a connection to a remote machine (i.e. ping(8) fails).

The traceroute(8) command is run with the name of the remote host you are trying to connect to. It will show the gateway hosts along the path of the attempt, eventually either reaching the target host, or terminating because of a lack of connection.

For more information, see the manual page for traceroute(8).

56.2.8. Multicast Routing

FreeBSD supports both multicast applications and multicast routing natively. Multicast applications do not require any special configuration of FreeBSD; applications will generally run out of the box. Multicast routing requires that support be compiled into the kernel:

```
options MROUTING
```

In addition, the multicast routing daemon, mrouted(8) must be configured to set up tunnels and DVMRP via /etc/mrouted.conf. More details on multicast configuration may be found in the manual page for mrouted(8).

56.3. Wireless Networking

56.3.1. Wireless Networking Basics

Most wireless networks are based on the IEEE 802.11 standards. A basic wireless network consists of multiple stations communicating with radios that broadcast in either the 2.4GHz or 5GHz band (though this varies according to the locale and is also changing to enable communication in the 2.3GHz and 4.9GHz ranges).

802.11 networks are organized in two ways: in *infrastructure mode* one station acts as a master with all the other stations associating to it; the network is known as a BSS and the master station is termed an access point (AP). In a BSS all communication passes through the AP; even when one station wants to communicate with another wireless station messages must go through the AP. In the second form of network there is no master and stations communicate directly. This form of network is termed an IBSS and is commonly known as an *ad-hoc network*.

802.11 networks were first deployed in the 2.4GHz band using protocols defined by the IEEE 802.11 and 802.11b standard. These specifications include the operating frequencies, MAC layer characteristics including framing and transmission rates (communication can be done at various rates). Later the 802.11a standard defined operation in the 5GHz band, including different

signalling mechanisms and higher transmission rates. Still later the 802.11g standard was defined to enable use of 802.11a signalling and transmission mechanisms in the 2.4GHz band in such a way as to be backwards compatible with 802.11b networks.

Separate from the underlying transmission techniques 802.11 networks have a variety of security mechanisms. The original 802.11 specifications defined a simple security protocol called WEP. This protocol uses a fixed pre-shared key and the RC4 cryptographic cipher to encode data transmitted on a network. Stations must all agree on the fixed key in order to communicate. This scheme was shown to be easily broken and is now rarely used except to discourage transient users from joining networks. Current security practice is given by the IEEE 802.11i specification that defines new cryptographic ciphers and an additional protocol to authenticate stations to an access point and exchange keys for doing data communication. Further, cryptographic keys are periodically refreshed and there are mechanisms for detecting intrusion attempts (and for countering intrusion attempts). Another security protocol specification commonly used in wireless networks is termed WPA. This was a precursor to 802.11i defined by an industry group as an interim measure while waiting for 802.11i to be ratified. WPA specifies a subset of the requirements found in 802.11i and is designed for implementation on legacy hardware. Specifically WPA requires only the TKIP cipher that is derived from the original WEP cipher. 802.11i permits use of TKIP but also requires support for a stronger cipher, AES-CCM, for encrypting data. (The AES cipher was not required in WPA because it was deemed too computationally costly to be implemented on legacy hardware.)

Other than the above protocol standards the other important standard to be aware of is 802.11e. This defines protocols for deploying multi-media applications such as streaming video and voice over IP (VoIP) in an 802.11 network. Like 802.11i, 802.11e also has a precursor specification termed WME (later renamed WMM) that has been defined by an industry group as a subset of 802.11e that can be deployed now to enable multi-media applications while waiting for the final ratification of 802.11e. The most important thing to know about 802.11e and WME/WMM is that it enables prioritized traffic use of a wireless network through Quality of Service (QoS) protocols and enhanced media access protocols. Proper implementation of these protocols enable high speed bursting of data and prioritized traffic flow.

Since the 6.0 version, FreeBSD supports networks that operate using 802.11a, 802.11b, and 802.11g. The WPA and 802.11i security protocols are likewise supported (in conjunction with any of 11a, 11b, and 11g) and QoS and traffic prioritization required by the WME/WMM protocols are supported for a limited set of wireless devices.

56.3.2. Basic Setup

56.3.2.1. Kernel Configuration

To use wireless networking you need a wireless networking card and to configure the kernel with the appropriate wireless networking support. The latter is separated into multiple modules so that you only need to configure the software you are actually going to use.

The first thing you need is a wireless device. The most commonly used devices are those that use parts made by Atheros. These devices are supported by the ath(4) driver and require the following line to be added to the /boot/loader.conf file:

```
if_ath_load="YES"
```

The Atheros driver is split up into three separate pieces: the driver proper (ath(4)), the hardware support layer that handles chip-specific functions (ath_hal(4)), and an algorithm for selecting which of several possible rates for transmitting frames (ath_rate_sample here). When you load this support as modules these dependencies are automatically handled for you. If instead of an Atheros device you had another device you would select the module for that device; e.g.:

```
if_wi_load="YES"
```

for devices based on the Intersil Prism parts (wi(4) driver).

In the rest of this document, we will use an ath(4) device, the device name in the examples must be changed according to your configuration. A list of available wireless drivers can be found at the beginning of the wlan(4) manual page. If a native FreeBSD driver for your wireless device does not exist, it may be possible to directly use the Windows® driver with the help of the NDIS driver wrapper.

With a device driver configured you need to also bring in the 802.11 networking support required by the driver. For the ath(4) driver this is at least the wlan(4) module; this module is automatically loaded with the wireless device driver. With that you will need the modules that implement cryptographic support for the security protocols you intend to use. These are intended to be dynamically loaded on demand by the wlan(4) module but for now they must be manually configured. The following modules are available: wlan_wep(4), wlan_ccmp(4) and wlan_tkip(4). Both wlan_ccmp(4) and wlan_tkip(4) drivers are only needed if you intend to use the WPA and/or 802.11i security protocols. If your network is to run totally open (i.e., with no encryption) then you do not even need the wlan_wep(4) support. To load these modules at boot time, add the following lines to /boot/loader.conf:

```
wlan_wep_load="YES"
wlan_ccmp_load="YES"
wlan_tkip_load="YES"
```

With this information in the system bootstrap configuration file (i.e., /boot/loader.conf), you have to reboot your FreeBSD box. If you do not want to reboot your machine for the moment, you can just load the modules by hand using kldload(8).

If you do not want to use modules, it is possible to compile these drivers into the kernel by adding the following lines to your kernel configuration file:

```
device ath               # Atheros IEEE 802.11 wireless network driver
device ath_hal           # Atheros Hardware Access Layer
device ath_rate_sample   # John Bicket's SampleRate control algorithm.
device wlan              # 802.11 support (Required)
device wlan_wep          # WEP crypto support for 802.11 devices
```

```
device wlan_ccmp         # AES-CCMP crypto support for 802.11 devices
device wlan_tkip         # TKIP and Michael crypto support for 802.11
devices
```

With this information in the kernel configuration file, recompile the kernel and reboot your FreeBSD machine.

When the system is up, we could find some information about the wireless device in the boot messages, like this:

```
ath0: <Atheros 5212> mem 0xff9f0000-0xff9fffff irq 17 at device 2.0 on pci2
ath0: Ethernet address: 00:11:95:d5:43:62
ath0: mac 7.9 phy 4.5 radio 5.6
```

56.3.3. Infrastructure Mode

The infrastructure mode or BSS mode is the mode that is typically used. In this mode, a number of wireless access points are connected to a wired network. Each wireless network has its own name, this name is called the SSID of the network. Wireless clients connect to the wireless access points.

56.3.3.1. FreeBSD Clients

56.3.3.1.1. How to Find Access Points

To scan for networks, use the `ifconfig` command. This request may take a few moments to complete as it requires that the system switches to each available wireless frequency and probes for available access points. Only the super-user can initiate such a scan:

```
# ifconfig ath0 up scan
SSID            BSSID              CHAN RATE  S:N   INT CAPS
dlinkap         00:13:46:49:41:76    6   54M 29:0   100 EPS  WPA WME
freebsdap       00:11:95:c3:0d:ac    1   54M 22:0   100 EPS  WPA
```

You must mark the interface `up` before you can scan. Subsequent scan requests do not require you to mark the interface up again.

The output of a scan request lists each BSS/IBSS network found. Beside the name of the network, `SSID`, we find the `BSSID` which is the MAC address of the access point. The `CAPS` field identifies the type of each network and the capabilities of the stations operating there:

`E`

Extended Service Set (ESS). Indicates that the station is part of an infrastructure network (in contrast to an IBSS/ad-hoc network).

`I`

IBSS/ad-hoc network. Indicates that the station is part of an ad-hoc network (in contrast to an

ESS network).

`P`

Privacy. Data confidentiality is required for all data frames exchanged within the BSS. This means that this BSS requires the station to use cryptographic means such as WEP, TKIP or AES-CCMP to encrypt/decrypt data frames being exchanged with others.

`S`

Short Preamble. Indicates that the network is using short preambles (defined in 802.11b High Rate/DSSS PHY, short preamble utilizes a 56 bit sync field in contrast to a 128 bit field used in long preamble mode).

`s`

Short slot time. Indicates that the 802.11g network is using a short slot time because there are no legacy (802.11b) stations present.

One can also display the current list of known networks with:

```
# ifconfig ath0 list scan
```

This information may be updated automatically by the adapter or manually with a `scan` request. Old data is automatically removed from the cache, so over time this list may shrink unless more scans are done.

56.3.3.1.2. Basic Settings

This section provides a simple example of how to make the wireless network adapter work in FreeBSD without encryption. After you are familiar with these concepts, we strongly recommend using WPA to set up your wireless network.

There are three basic steps to configure a wireless network: selecting an access point, authenticating your station, and configuring an IP address. The following sections discuss each step.

56.3.3.1.2.1. Selecting an Access Point

Most of time it is sufficient to let the system choose an access point using the builtin heuristics. This is the default behaviour when you mark an interface up or otherwise configure an interface by listing it in /etc/rc.conf, e.g.:

```
ifconfig_ath0="DHCP"
```

If there are multiple access points and you want to select a specific one, you can select it by its SSID:

```
ifconfig_ath0="ssid your_ssid_here DHCP"
```

In an environment where there are multiple access points with the same SSID (often done to

simplify roaming) it may be necessary to associate to one specific device. In this case you can also specify the BSSID of the access point (you can also leave off the SSID):

```
ifconfig_ath0="ssid your_ssid_here bssid xx:xx:xx:xx:xx:xx DHCP"
```

There are other ways to constrain the choice of an access point such as limiting the set of frequencies the system will scan on. This may be useful if you have a multi-band wireless card as scanning all the possible channels can be time-consuming. To limit operation to a specific band you can use the `mode` parameter; e.g.:

```
ifconfig_ath0="mode 11g ssid your_ssid_here DHCP"
```

will force the card to operate in 802.11g which is defined only for 2.4GHz frequencies so any 5GHz channels will not be considered. Other ways to do this are the `channel` parameter, to lock operation to one specific frequency, and the `chanlist` parameter, to specify a list of channels for scanning. More information about these parameters can be found in the ifconfig(8) manual page.

56.3.3.1.2.2. Authentication

Once you have selected an access point your station needs to authenticate before it can pass data. Authentication can happen in several ways. The most common scheme used is termed open authentication and allows any station to join the network and communicate. This is the authentication you should use for test purpose the first time you set up a wireless network. Other schemes require cryptographic handshakes be completed before data traffic can flow; either using pre-shared keys or secrets, or more complex schemes that involve backend services such as RADIUS. Most users will use open authentication which is the default setting. Next most common setup is WPA-PSK, also known as WPA Personal, which is described below.

If you have an Apple® AirPort® Extreme base station for an access point you may need to configure shared-key authentication together with a WEP key. This can be done in the /etc/rc.conf file or using the wpa_supplicant(8) program. If you have a single AirPort® base station you can setup access with something like:

```
ifconfig_ath0="authmode shared wepmode on weptxkey 1 wepkey 01234567
DHCP"
```

In general shared key authentication is to be avoided because it uses the WEP key material in a highly-constrained manner making it even easier to crack the key. If WEP must be used (e.g., for compatibility with legacy devices) it is better to use WEP with `open` authentication. More information regarding WEP can be found in the WEP.

56.3.3.1.2.3. Getting an IP Address with DHCP

Once you have selected an access point and set the authentication parameters, you will have to get an IP address to communicate. Most of time you will obtain your wireless IP address via DHCP. To

achieve that, simply edit /etc/rc.conf and add DHCP to the configuration for your device as shown in various examples above:

```
ifconfig_ath0="DHCP"
```

At this point, you are ready to bring up the wireless interface:

```
# /etc/rc.d/netif start
```

Once the interface is running, use ifconfig to see the status of the interface ath0:

```
# ifconfig ath0
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
        inet 192.168.1.100 netmask 0xffffff00 broadcast 192.168.1.255
        ether 00:11:95:d5:43:62
        media: IEEE 802.11 Wireless Ethernet autoselect (OFDM/54Mbps)
        status: associated
        ssid dlinkap channel 6 bssid 00:13:46:49:41:76
        authmode OPEN privacy OFF txpowmax 36 protmode CTS bintval 100
```

The status: associated means you are connected to the wireless network (to the dlinkap network in our case). The bssid 00:13:46:49:41:76 part is the MAC address of your access point; the authmode line informs you that the communication is not encrypted (OPEN).

56.3.3.1.2.4. Static IP Address

In the case you cannot obtain an IP address from a DHCP server, you can set a fixed IP address. Replace the DHCP keyword shown above with the address information. Be sure to retain any other parameters you have set up for selecting an access point:

```
ifconfig_ath0="inet 192.168.1.100 netmask 255.255.255.0 ssid your_ssid_here"
```

56.3.3.1.3. WPA

WPA (Wi-Fi Protected Access) is a security protocol used together with 802.11 networks to address the lack of proper authentication and the weakness of WEP. WPA leverages the 802.1X authentication protocol and uses one of several ciphers instead of WEP for data integrity. The only cipher required by WPA is TKIP (Temporary Key Integrity Protocol) which is a cipher that extends the basic RC4 cipher used by WEP by adding integrity checking, tamper detection, and measures for responding to any detected intrusions. TKIP is designed to work on legacy hardware with only software modification; it represents a compromise that improves security but is still not entirely immune to attack. WPA also specifies the AES-CCMP cipher as an alternative to TKIP and that is preferred when possible; for this specification the term WPA2 (or RSN) is commonly used.

WPA defines authentication and encryption protocols. Authentication is most commonly done

using one of two techniques: by 802.1X and a backend authentication service such as RADIUS, or by a minimal handshake between the station and the access point using a pre-shared secret. The former is commonly termed WPA Enterprise with the latter known as WPA Personal. Since most people will not set up a RADIUS backend server for wireless network, WPA-PSK is by far the most commonly encountered configuration for WPA.

The control of the wireless connection and the authentication (key negotiation or authentication with a server) is done with the wpa_supplicant(8) utility. This program requires a configuration file, /etc/wpa_supplicant.conf, to run. More information regarding this file can be found in the wpa_supplicant.conf(5) manual page.

56.3.3.1.3.1. WPA-PSK

WPA-PSK also known as WPA-Personal is based on a pre-shared key (PSK) generated from a given password and that will be used as the master key in the wireless network. This means every wireless user will share the same key. WPA-PSK is intended for small networks where the use of an authentication server is not possible or desired.

Always use strong passwords that are sufficiently long and made from a rich alphabet so they will not be guessed and/or attacked.

The first step is the configuration of the /etc/wpa_supplicant.conf file with the SSID and the pre-shared key of your network:

```
network={
  ssid="freebsdap"
  psk="freebsdmall"
}
```

Then, in /etc/rc.conf, we indicate that the wireless device configuration will be done with WPA and the IP address will be obtained with DHCP:

```
ifconfig_ath0="WPA DHCP"
```

Then, we can bring up the interface:

```
# /etc/rc.d/netif start
Starting wpa_supplicant.
DHCPDISCOVER on ath0 to 255.255.255.255 port 67 interval 5
DHCPDISCOVER on ath0 to 255.255.255.255 port 67 interval 6
DHCPOFFER from 192.168.0.1
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.1
bound to 192.168.0.254 -- renewal in 300 seconds.
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
      inet 192.168.0.254 netmask 0xffffff00 broadcast 192.168.0.255
```

```
        ether 00:11:95:d5:43:62
        media: IEEE 802.11 Wireless Ethernet autoselect (OFDM/36Mbps)
        status: associated
        ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
        authmode WPA privacy ON deftxkey UNDEF TKIP 2:128-bit txpowmax 36
        protmode CTS roaming MANUAL bintval 100
```

Or you can try to configure it manually using the same /etc/wpa_supplicant.conf above, and run:

```
# wpa_supplicant -i ath0 -c /etc/wpa_supplicant.conf
Trying to associate with 00:11:95:c3:0d:ac (SSID='freebsdap' freq=2412 MHz)
Associated with 00:11:95:c3:0d:ac
WPA: Key negotiation completed with 00:11:95:c3:0d:ac [PTK=TKIP GTK=TKIP]
```

The next operation is the launch of the `dhclient` command to get the IP address from the DHCP server:

```
# dhclient ath0
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.1
bound to 192.168.0.254 -- renewal in 300 seconds.
# ifconfig ath0
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
        inet 192.168.0.254 netmask 0xffffff00 broadcast 192.168.0.255
        ether 00:11:95:d5:43:62
        media: IEEE 802.11 Wireless Ethernet autoselect (OFDM/48Mbps)
        status: associated
        ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
        authmode WPA privacy ON deftxkey UNDEF TKIP 2:128-bit txpowmax 36
        protmode CTS roaming MANUAL bintval 100
```

If the /etc/rc.conf is set up with the line `ifconfig_ath0="DHCP"` then it is no need to run the `dhclient` command manually, `dhclient` will be launched after `wpa_supplicant` plumbs the keys.

In the case where the use of DHCP is not possible, you can set a static IP address after `wpa_supplicant` has authenticated the station:

```
# ifconfig ath0 inet 192.168.0.100 netmask 255.255.255.0
# ifconfig ath0
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
        inet 192.168.0.100 netmask 0xffffff00 broadcast 192.168.0.255
        ether 00:11:95:d5:43:62
        media: IEEE 802.11 Wireless Ethernet autoselect (OFDM/36Mbps)
        status: associated
```

```
        ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
        authmode WPA privacy ON deftxkey UNDEF TKIP 2:128-bit txpowmax 36
        protmode CTS roaming MANUAL bintval 100
```

When DHCP is not used, you also have to manually set up the default gateway and the nameserver:

```
# route add default your_default_router
# echo "nameserver your_DNS_server" >> /etc/resolv.conf
```

56.3.3.1.3.2. WPA with EAP-TLS

The second way to use WPA is with an 802.1X backend authentication server, in this case WPA is called WPA-Enterprise to make difference with the less secure WPA-Personal with its pre-shared key. The authentication in WPA-Enterprise is based on EAP (Extensible Authentication Protocol).

EAP does not come with an encryption method, it was decided to embed EAP inside an encrypted tunnel. Many types of EAP authentication methods have been designed, the most common methods are EAP-TLS, EAP-TTLS and EAP-PEAP.

EAP-TLS (EAP with Transport Layer Security) is a very well-supported authentication protocol in the wireless world since it was the first EAP method to be certified by the Wi-Fi alliance. EAP-TLS will require three certificates to run: the CA certificate (installed on all machines), the server certificate for your authentication server, and one client certificate for each wireless client. In this EAP method, both authentication server and wireless client authenticate each other in presenting their respective certificates, and they verify that these certificates were signed by your organization's certificate authority (CA).

As previously, the configuration is done via /etc/wpa_supplicant.conf:

```
network={
  ssid="freebsdap" ①
  proto=RSN  ②
  key_mgmt=WPA-EAP ③
  eap=TLS ④
  identity="loader" ⑤
  ca_cert="/etc/certs/cacert.pem" ⑥
  client_cert="/etc/certs/clientcert.pem" ⑦
  private_key="/etc/certs/clientkey.pem" ⑧
  private_key_passwd="freebsdmallclient" ⑨
}
```

① This field indicates the network name (SSID).

② Here, we use RSN (IEEE 802.11i) protocol, i.e., WPA2.

③ The `key_mgmt` line refers to the key management protocol we use. In our case it is WPA using EAP authentication: `WPA-EAP`.

④ In this field, we mention the EAP method for our connection.

⑤ The `identity` field contains the identity string for EAP.

⑥ The `ca_cert` field indicates the pathname of the CA certificate file. This file is needed to verify the server certificat.

⑦ The `client_cert` line gives the pathname to the client certificate file. This certificate is unique to each wireless client of the network.

⑧ The `private_key` field is the pathname to the client certificate private key file.

⑨ The `private_key_passwd` field contains the passphrase for the private key.

Then add the following line to /etc/rc.conf:

```
ifconfig_ath0="WPA DHCP"
```

The next step is to bring up the interface with the help of the rc.d facility:

```
# /etc/rc.d/netif start
Starting wpa_supplicant.
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.20
bound to 192.168.0.254 -- renewal in 300 seconds.
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
      inet 192.168.0.254 netmask 0xffffff00 broadcast 192.168.0.255
      ether 00:11:95:d5:43:62
      media: IEEE 802.11 Wireless Ethernet autoselect (DS/11Mbps)
      status: associated
      ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
      authmode WPA2/802.11i privacy ON deftxkey UNDEF TKIP 2:128-bit
      txpowmax 36 protmode CTS roaming MANUAL bintval 100
```

As previously shown, it is also possible to bring up the interface manually with both `wpa_supplicant` and `ifconfig` commands.

56.3.3.1.3.3. WPA with EAP-TTLS

With EAP-TLS both the authentication server and the client need a certificate, with EAP-TTLS (EAP-Tunneled Transport Layer Security) a client certificate is optional. This method is close to what some secure web sites do , where the web server can create a secure SSL tunnel even if the visitors do not have client-side certificates. EAP-TTLS will use the encrypted TLS tunnel for safe transport of the authentication data.

The configuration is done via the /etc/wpa_supplicant.conf file:

```
network={
  ssid="freebsdap"
  proto=RSN
```

```
  key_mgmt=WPA-EAP
  eap=TTLS ①
  identity="test" ②
  password="test" ③
  ca_cert="/etc/certs/cacert.pem" ④
  phase2="auth=MD5" ⑤
}
```

① In this field, we mention the EAP method for our connection.

② The `identity` field contains the identity string for EAP authentication inside the encrypted TLS tunnel.

③ The `password` field contains the passphrase for the EAP authentication.

④ The `ca_cert` field indicates the pathname of the CA certificate file. This file is needed to verify the server certificat.

⑤ In this field, we mention the authentication method used in the encrypted TLS tunnel. In our case, EAP with MD5-Challenge has been used. The "inner authentication" phase is often called "phase2".

You also have to add the following line to /etc/rc.conf:

```
ifconfig_ath0="WPA DHCP"
```

The next step is to bring up the interface:

```
# /etc/rc.d/netif start
Starting wpa_supplicant.
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.20
bound to 192.168.0.254 -- renewal in 300 seconds.
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
      inet 192.168.0.254 netmask 0xffffff00 broadcast 192.168.0.255
      ether 00:11:95:d5:43:62
      media: IEEE 802.11 Wireless Ethernet autoselect (DS/11Mbps)
      status: associated
      ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
      authmode WPA2/802.11i privacy ON deftxkey UNDEF TKIP 2:128-bit
      txpowmax 36 protmode CTS roaming MANUAL bintval 100
```

56.3.3.1.3.4. WPA with EAP-PEAP

PEAP (Protected EAP) has been designed as an alternative to EAP-TTLS. There are two types of PEAP methods, the most common one is PEAPv0/EAP-MSCHAPv2. In the rest of this document, we will use the PEAP term to refer to that EAP method. PEAP is the most used EAP standard after EAP-TLS, in

other words if you have a network with mixed OSes, PEAP should be the most supported standard after EAP-TLS.

PEAP is similar to EAP-TTLS: it uses a server-side certificate to authenticate clients by creating an encrypted TLS tunnel between the client and the authentication server, which protects the ensuing exchange of authentication information. In term of security the difference between EAP-TTLS and PEAP is that PEAP authentication broadcasts the username in clear, only the password is sent in the encrypted TLS tunnel. EAP-TTLS will use the TLS tunnel for both username and password.

We have to edit the /etc/wpa_supplicant.conf file and add the EAP-PEAP related settings:

```
network={
  ssid="freebsdap"
  proto=RSN
  key_mgmt=WPA-EAP
  eap=PEAP ①
  identity="test" ②
  password="test" ③
  ca_cert="/etc/certs/cacert.pem" ④
  phase1="peaplabel=0" ⑤
  phase2="auth=MSCHAPV2" ⑥
}
```

① In this field, we mention the EAP method for our connection.

② The `identity` field contains the identity string for EAP authentication inside the encrypted TLS tunnel.

③ The `password` field contains the passphrase for the EAP authentication.

④ The `ca_cert` field indicates the pathname of the CA certificate file. This file is needed to verify the server certificat.

⑤ This field contains the parameters for the first phase of the authentication (the TLS tunnel). According to the authentication server used, you will have to specify a specific label for the authentication. Most of time, the label will be "client EAP encryption" which is set by using `peaplabel=0`. More information can be found in the wpa_supplicant.conf(5) manual page.

⑥ In this field, we mention the authentication protocol used in the encrypted TLS tunnel. In the case of PEAP, it is `auth=MSCHAPV2`.

The following must be added to /etc/rc.conf:

```
ifconfig_ath0="WPA DHCP"
```

Then, we can bring up the interface:

```
# /etc/rc.d/netif start
Starting wpa_supplicant.
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPREQUEST on ath0 to 255.255.255.255 port 67
```

```
DHCPREQUEST on ath0 to 255.255.255.255 port 67
DHCPACK from 192.168.0.20
bound to 192.168.0.254 -- renewal in 300 seconds.
ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
      inet 192.168.0.254 netmask 0xffffff00 broadcast 192.168.0.255
      ether 00:11:95:d5:43:62
      media: IEEE 802.11 Wireless Ethernet autoselect (DS/11Mbps)
      status: associated
      ssid freebsdap channel 1 bssid 00:11:95:c3:0d:ac
      authmode WPA2/802.11i privacy ON deftxkey UNDEF TKIP 2:128-bit
      txpowmax 36 protmode CTS roaming MANUAL bintval 100
```

56.3.3.1.4. WEP

WEP (Wired Equivalent Privacy) is part of the original 802.11 standard. There is no authentication mechanism, only a weak form of access control, and it is easily to be cracked.

WEP can be set up with `ifconfig`:

```
# ifconfig ath0 inet 192.168.1.100 netmask 255.255.255.0 ssid my_net \
        wepmode on weptxkey 3 wepkey 3:0x3456789012
```

- The `weptxkey` means which WEP key will be used in the transmission. Here we used the third key. This must match the setting in the access point.
- The `wepkey` means setting the selected WEP key. It should in the format *index:key*, if the index is not given, key `1` is set. That is to say we need to set the index if we use keys other than the first key.

You must replace the `0x3456789012` with the key configured for use on the access point.

You are encouraged to read ifconfig(8) manual page for further information.

The `wpa_supplicant` facility also can be used to configure your wireless interface with WEP. The example above can be set up by adding the following lines to /etc/wpa_supplicant.conf:

```
network={
  ssid="my_net"
  key_mgmt=NONE
  wep_key3=3456789012
  wep_tx_keyidx=3
}
```

Then:

```
# wpa_supplicant -i ath0 -c /etc/wpa_supplicant.conf
```

```
Trying to associate with 00:13:46:49:41:76 (SSID='dlinkap' freq=2437 MHz)
Associated with 00:13:46:49:41:76
```

56.3.4. Ad-hoc Mode

IBSS mode, also called ad-hoc mode, is designed for point to point connections. For example, to establish an ad-hoc network between the machine A and the machine B we will just need to choose two IP adresses and a SSID.

On the box A:

```
# ifconfig ath0 inet 192.168.0.1 netmask 255.255.255.0 ssid freebsdap mediaopt adhoc
# ifconfig ath0
  ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet 192.168.0.1 netmask 0xffffff00 broadcast 192.168.0.255
      inet6 fe80::211:95ff:fec3:dac%ath0 prefixlen 64 scopeid 0x4
      ether 00:11:95:c3:0d:ac
      media: IEEE 802.11 Wireless Ethernet autoselect <adhoc> (autoselect <adhoc>)
      status: associated
      ssid freebsdap channel 2 bssid 02:11:95:c3:0d:ac
      authmode OPEN privacy OFF txpowmax 36 protmode CTS bintval 100
```

The adhoc parameter indicates the interface is running in the IBSS mode.

On B, we should be able to detect A:

```
# ifconfig ath0 up scan
  SSID            BSSID              CHAN RATE  S:N   INT CAPS
  freebsdap       02:11:95:c3:0d:ac    2   54M 19:0   100 IS
```

The I in the output confirms the machine A is in ad-hoc mode. We just have to configure B with a different IP address:

```
# ifconfig ath0 inet 192.168.0.2 netmask 255.255.255.0 ssid freebsdap mediaopt adhoc
# ifconfig ath0
  ath0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
      inet6 fe80::211:95ff:fed5:4362%ath0 prefixlen 64 scopeid 0x1
      inet 192.168.0.2 netmask 0xffffff00 broadcast 192.168.0.255
      ether 00:11:95:d5:43:62
      media: IEEE 802.11 Wireless Ethernet autoselect <adhoc> (autoselect <adhoc>)
      status: associated
      ssid freebsdap channel 2 bssid 02:11:95:c3:0d:ac
      authmode OPEN privacy OFF txpowmax 36 protmode CTS bintval 100
```

Both A and B are now ready to exchange informations.

56.3.5. Troubleshooting

If you are having trouble with wireless networking, there are a number of steps you can take to help troubleshoot the problem.

- If you do not see the access point listed when scanning be sure you have not configured your wireless device to a limited set of channels.
- If you cannot associate to an access point verify the configuration of your station matches the one of the access point. This includes the authentication scheme and any security protocols. Simplify your configuration as much as possible. If you are using a security protocol such as WPA or WEP configure the access point for open authentication and no security to see if you can get traffic to pass.
- Once you can associate to the access point diagnose any security configuration using simple tools like ping(8).

  The `wpa_supplicant` has much debugging support; try running it manually with the `-dd` option and look at the system logs.

- There are also many lower-level debugging tools. You can enable debugging messages in the 802.11 protocol support layer using the `wlandebug` program found in /usr/src/tools/tools/net80211. For example:

  ```
  # wlandebug -i ath0 +scan+auth+debug+assoc
    net.wlan.0.debug: 0 => 0xc80000<assoc,auth,scan>
  ```

  can be used to enable console messages related to scanning for access points and doing the 802.11 protocol handshakes required to arrange communication.

  There are also many useful statistics maintained by the 802.11 layer; the `wlanstats` tool will dump these informations. These statistics should identify all errors identified by the 802.11 layer. Beware however that some errors are identified in the device drivers that lie below the 802.11 layer so they may not show up. To diagnose device-specific problems you need to refer to the drivers' documentation.

If the above information does not help to clarify the problem, please submit a problem report and include output from the above tools.

56.4. Bluetooth

56.4.1. Introduction

Bluetooth is a wireless technology for creating personal networks operating in the 2.4 GHz unlicensed band, with a range of 10 meters. Networks are usually formed ad-hoc from portable devices such as cellular phones, handhelds and laptops. Unlike the other popular wireless technology, Wi-Fi, Bluetooth offers higher level service profiles, e.g. FTP-like file servers, file pushing, voice transport, serial line emulation, and more.

The Bluetooth stack in FreeBSD is implemented using the Netgraph framework (see netgraph(4)). A broad variety of Bluetooth USB dongles is supported by the ng_ubt(4) driver. The Broadcom BCM2033 chip based Bluetooth devices are supported via the ubtbcmfw(4) and ng_ubt(4) drivers. The 3Com Bluetooth PC Card 3CRWB60-A is supported by the ng_bt3c(4) driver. Serial and UART based Bluetooth devices are supported via sio(4), ng_h4(4) and hcseriald(8). This section describes the use of the USB Bluetooth dongle.

56.4.2. Plugging in the Device

By default Bluetooth device drivers are available as kernel modules. Before attaching a device, you will need to load the driver into the kernel:

```
# kldload ng_ubt
```

If the Bluetooth device is present in the system during system startup, load the module from /boot/loader.conf:

```
ng_ubt_load="YES"
```

Plug in your USB dongle. The output similar to the following will appear on the console (or in syslog):

```
ubt0: vendor 0x0a12 product 0x0001, rev 1.10/5.25, addr 2
ubt0: Interface 0 endpoints: interrupt=0x81, bulk-in=0x82, bulk-out=0x2
ubt0: Interface 1 (alt.config 5) endpoints: isoc-in=0x83, isoc-out=0x3,
      wMaxPacketSize=49, nframes=6, buffer size=294
```

The Bluetooth stack has to be started manually on FreeBSD 6.0, and on FreeBSD 5.X before 5.5. It is done automatically from devd(8) on FreeBSD 5.5, 6.1 and newer.

Copy /usr/shared/examples/netgraph/bluetooth/rc.bluetooth into some convenient place, like /etc/rc.bluetooth. This script is used to start and stop the Bluetooth stack. It is a good idea to stop the stack before unplugging the device, but it is not (usually) fatal. When starting the stack, you will receive output similar to the following:

```
# /etc/rc.bluetooth start ubt0
BD_ADDR: 00:02:72:00:d4:1a
Features: 0xff 0xff 0xf 00 00 00 00 00
<3-Slot> <5-Slot> <Encryption> <Slot offset>
<Timing accuracy> <Switch> <Hold mode> <Sniff mode>
<Park mode> <RSSI> <Channel quality> <SCO link>
<HV2 packets> <HV3 packets> <u-law log> <A-law log> <CVSD>
<Paging scheme> <Power control> <Transparent SCO data>
Max. ACL packet size: 192 bytes
```

```
Number of ACL packets: 8
Max. SCO packet size: 64 bytes
Number of SCO packets: 8
```

56.4.3. Host Controller Interface (HCI)

Host Controller Interface (HCI) provides a command interface to the baseband controller and link manager, and access to hardware status and control registers. This interface provides a uniform method of accessing the Bluetooth baseband capabilities. HCI layer on the Host exchanges data and commands with the HCI firmware on the Bluetooth hardware. The Host Controller Transport Layer (i.e. physical bus) driver provides both HCI layers with the ability to exchange information with each other.

A single Netgraph node of type *hci* is created for a single Bluetooth device. The HCI node is normally connected to the Bluetooth device driver node (downstream) and the L2CAP node (upstream). All HCI operations must be performed on the HCI node and not on the device driver node. Default name for the HCI node is "devicehci". For more details refer to the ng_hci(4) manual page.

One of the most common tasks is discovery of Bluetooth devices in RF proximity. This operation is called *inquiry*. Inquiry and other HCI related operations are done with the hccontrol(8) utility. The example below shows how to find out which Bluetooth devices are in range. You should receive the list of devices in a few seconds. Note that a remote device will only answer the inquiry if it put into *discoverable* mode.

```
% hccontrol -n ubt0hci inquiry
Inquiry result, num_responses=1
Inquiry result #0
       BD_ADDR: 00:80:37:29:19:a4
       Page Scan Rep. Mode: 0x1
       Page Scan Period Mode: 00
       Page Scan Mode: 00
       Class: 52:02:04
       Clock offset: 0x78ef
Inquiry complete. Status: No error [00]
```

BD_ADDR is unique address of a Bluetooth device, similar to MAC addresses of a network card. This address is needed for further communication with a device. It is possible to assign human readable name to a BD_ADDR. The /etc/bluetooth/hosts file contains information regarding the known Bluetooth hosts. The following example shows how to obtain human readable name that was assigned to the remote device:

```
% hccontrol -n ubt0hci remote_name_request 00:80:37:29:19:a4
BD_ADDR: 00:80:37:29:19:a4
Name: Pav's T39
```

If you perform an inquiry on a remote Bluetooth device, it will find your computer as "your.host.name (ubt0)". The name assigned to the local device can be changed at any time.

The Bluetooth system provides a point-to-point connection (only two Bluetooth units involved), or a point-to-multipoint connection. In the point-to-multipoint connection the connection is shared among several Bluetooth devices. The following example shows how to obtain the list of active baseband connections for the local device:

```
% hccontrol -n ubt0hci read_connection_list
Remote BD_ADDR    Handle Type Mode Role Encrypt Pending Queue State
00:80:37:29:19:a4     41  ACL    0 MAST    NONE       0     0 OPEN
```

A *connection handle* is useful when termination of the baseband connection is required. Note, that it is normally not required to do it by hand. The stack will automatically terminate inactive baseband connections.

```
# hccontrol -n ubt0hci disconnect 41
Connection handle: 41
Reason: Connection terminated by local host [0x16]
```

Refer to `hccontrol help` for a complete listing of available HCI commands. Most of the HCI commands do not require superuser privileges.

56.4.4. Logical Link Control and Adaptation Protocol (L2CAP)

Logical Link Control and Adaptation Protocol (L2CAP) provides connection-oriented and connectionless data services to upper layer protocols with protocol multiplexing capability and segmentation and reassembly operation. L2CAP permits higher level protocols and applications to transmit and receive L2CAP data packets up to 64 kilobytes in length.

L2CAP is based around the concept of *channels*. Channel is a logical connection on top of baseband connection. Each channel is bound to a single protocol in a many-to-one fashion. Multiple channels can be bound to the same protocol, but a channel cannot be bound to multiple protocols. Each L2CAP packet received on a channel is directed to the appropriate higher level protocol. Multiple channels can share the same baseband connection.

A single Netgraph node of type *l2cap* is created for a single Bluetooth device. The L2CAP node is normally connected to the Bluetooth HCI node (downstream) and Bluetooth sockets nodes (upstream). Default name for the L2CAP node is "devicel2cap". For more details refer to the ng_l2cap(4) manual page.

A useful command is l2ping(8), which can be used to ping other devices. Some Bluetooth implementations might not return all of the data sent to them, so `0 bytes` in the following example is normal.

```
# l2ping -a 00:80:37:29:19:a4
0 bytes from 0:80:37:29:19:a4 seq_no=0 time=48.633 ms result=0
```

```
0 bytes from 0:80:37:29:19:a4 seq_no=1 time=37.551 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=2 time=28.324 ms result=0
0 bytes from 0:80:37:29:19:a4 seq_no=3 time=46.150 ms result=0
```

The l2control(8) utility is used to perform various operations on L2CAP nodes. This example shows how to obtain the list of logical connections (channels) and the list of baseband connections for the local device:

```
% l2control -a 00:02:72:00:d4:1a read_channel_list
L2CAP channels:
Remote BD_ADDR     SCID/ DCID   PSM  IMTU/ OMTU State
00:07:e0:00:0b:ca    66/   64     3   132/  672 OPEN
% l2control -a 00:02:72:00:d4:1a read_connection_list
L2CAP connections:
Remote BD_ADDR    Handle Flags Pending State
00:07:e0:00:0b:ca     41 O           0 OPEN
```

Another diagnostic tool is btsockstat(1). It does a job similar to as netstat(1) does, but for Bluetooth network-related data structures. The example below shows the same logical connection as l2control(8) above.

```
% btsockstat
Active L2CAP sockets
PCB      Recv-Q Send-Q Local address/PSM       Foreign address   CID   State
c2afe900      0      0 00:02:72:00:d4:1a/3     00:07:e0:00:0b:ca 66    OPEN
Active RFCOMM sessions
L2PCB    PCB      Flag MTU   Out-Q DLCs State
c2afe900 c2b53380 1    127   0     Yes  OPEN
Active RFCOMM sockets
PCB      Recv-Q Send-Q Local address     Foreign address   Chan DLCI State
c2e8bc80      0    250 00:02:72:00:d4:1a 00:07:e0:00:0b:ca 3    6    OPEN
```

56.4.5. RFCOMM Protocol

The RFCOMM protocol provides emulation of serial ports over the L2CAP protocol. The protocol is based on the ETSI standard TS 07.10. RFCOMM is a simple transport protocol, with additional provisions for emulating the 9 circuits of RS-232 (EIATIA-232-E) serial ports. The RFCOMM protocol supports up to 60 simultaneous connections (RFCOMM channels) between two Bluetooth devices.

For the purposes of RFCOMM, a complete communication path involves two applications running on different devices (the communication endpoints) with a communication segment between them. RFCOMM is intended to cover applications that make use of the serial ports of the devices in which they reside. The communication segment is a Bluetooth link from one device to another (direct connect).

RFCOMM is only concerned with the connection between the devices in the direct connect case, or between the device and a modem in the network case. RFCOMM can support other configurations,

such as modules that communicate via Bluetooth wireless technology on one side and provide a wired interface on the other side.

In FreeBSD the RFCOMM protocol is implemented at the Bluetooth sockets layer.

56.4.6. Pairing of Devices

By default, Bluetooth communication is not authenticated, and any device can talk to any other device. A Bluetooth device (for example, cellular phone) may choose to require authentication to provide a particular service (for example, Dial-Up service). Bluetooth authentication is normally done with *PIN codes*. A PIN code is an ASCII string up to 16 characters in length. User is required to enter the same PIN code on both devices. Once user has entered the PIN code, both devices will generate a *link key*. After that the link key can be stored either in the devices themselves or in a persistent storage. Next time both devices will use previously generated link key. The described above procedure is called *pairing*. Note that if the link key is lost by any device then pairing must be repeated.

The hcsecd(8) daemon is responsible for handling of all Bluetooth authentication requests. The default configuration file is /etc/bluetooth/hcsecd.conf. An example section for a cellular phone with the PIN code arbitrarily set to "1234" is shown below:

```
device {
        bdaddr  00:80:37:29:19:a4;
        name    "Pav's T39";
        key     nokey;
        pin     "1234";
      }
```

There is no limitation on PIN codes (except length). Some devices (for example Bluetooth headsets) may have a fixed PIN code built in. The `-d` switch forces the hcsecd(8) daemon to stay in the foreground, so it is easy to see what is happening. Set the remote device to receive pairing and initiate the Bluetooth connection to the remote device. The remote device should say that pairing was accepted, and request the PIN code. Enter the same PIN code as you have in hcsecd.conf. Now your PC and the remote device are paired. Alternatively, you can initiate pairing on the remote device.

On FreeBSD 5.5, 6.1 and newer, the following line can be added to the /etc/rc.conf file to have hcsecd started automatically on system start:

```
hcsecd_enable="YES"
```

The following is a sample of the hcsecd daemon output:

```
hcsecd[16484]: Got Link_Key_Request event from 'ubt0hci', remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39',
link key doesn't exist
```

```
hcsecd[16484]: Sending Link_Key_Negative_Reply to 'ubt0hci' for remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Got PIN_Code_Request event from 'ubt0hci', remote bdaddr
0:80:37:29:19:a4
hcsecd[16484]: Found matching entry, remote bdaddr 0:80:37:29:19:a4, name 'Pav's T39',
PIN code exists
hcsecd[16484]: Sending PIN_Code_Reply to 'ubt0hci' for remote bdaddr 0:80:37:29:19:a4
```

56.4.7. Service Discovery Protocol (SDP)

The Service Discovery Protocol (SDP) provides the means for client applications to discover the existence of services provided by server applications as well as the attributes of those services. The attributes of a service include the type or class of service offered and the mechanism or protocol information needed to utilize the service.

SDP involves communication between a SDP server and a SDP client. The server maintains a list of service records that describe the characteristics of services associated with the server. Each service record contains information about a single service. A client may retrieve information from a service record maintained by the SDP server by issuing a SDP request. If the client, or an application associated with the client, decides to use a service, it must open a separate connection to the service provider in order to utilize the service. SDP provides a mechanism for discovering services and their attributes, but it does not provide a mechanism for utilizing those services.

Normally, a SDP client searches for services based on some desired characteristics of the services. However, there are times when it is desirable to discover which types of services are described by an SDP server's service records without any a priori information about the services. This process of looking for any offered services is called *browsing*.

The Bluetooth SDP server sdpd(8) and command line client sdpcontrol(8) are included in the standard FreeBSD installation. The following example shows how to perform a SDP browse query.

```
% sdpcontrol -a 00:01:03:fc:6e:ec browse
Record Handle: 00000000
Service Class ID List:
        Service Discovery Server (0x1000)
Protocol Descriptor List:
        L2CAP (0x0100)
                Protocol specific parameter #1: u/int/uuid16 1
                Protocol specific parameter #2: u/int/uuid16 1

Record Handle: 0x00000001
Service Class ID List:
        Browse Group Descriptor (0x1001)

Record Handle: 0x00000002
Service Class ID List:
        LAN Access Using PPP (0x1102)
Protocol Descriptor List:
        L2CAP (0x0100)
```

```
        RFCOMM (0x0003)
                Protocol specific parameter #1: u/int8/bool 1
Bluetooth Profile Descriptor List:
        LAN Access Using PPP (0x1102) ver. 1.0
```

i. and so on. Note that each service has a list of attributes (RFCOMM channel for example). Depending on the service you might need to make a note of some of the attributes. Some Bluetooth implementations do not support service browsing and may return an empty list. In this case it is possible to search for the specific service. The example below shows how to search for the OBEX Object Push (OPUSH) service:

```
% sdpcontrol -a 00:01:03:fc:6e:ec search OPUSH
```

Offering services on FreeBSD to Bluetooth clients is done with the sdpd(8) server. On FreeBSD 5.5, 6.1 and newer, the following line can be added to the /etc/rc.conf file:

```
sdpd_enable="YES"
```

Then the sdpd daemon can be started with:

```
# /etc/rc.d/sdpd start
```

On FreeBSD 6.0, and on FreeBSD 5.X before 5.5, sdpd is not integrated into the system startup scripts. It has to be started manually with:

```
# sdpd
```

The local server application that wants to provide Bluetooth service to the remote clients will register service with the local SDP daemon. The example of such application is rfcomm_pppd(8). Once started it will register Bluetooth LAN service with the local SDP daemon.

The list of services registered with the local SDP server can be obtained by issuing SDP browse query via local control channel:

```
# sdpcontrol -l browse
```

56.4.8. Dial-Up Networking (DUN) and Network Access with PPP (LAN) Profiles

The Dial-Up Networking (DUN) profile is mostly used with modems and cellular phones. The scenarios covered by this profile are the following:

- use of a cellular phone or modem by a computer as a wireless modem for connecting to a dial-

up Internet access server, or using other dial-up services;

- use of a cellular phone or modem by a computer to receive data calls.

Network Access with PPP (LAN) profile can be used in the following situations:

- LAN access for a single Bluetooth device;
- LAN access for multiple Bluetooth devices;
- PC to PC (using PPP networking over serial cable emulation).

In FreeBSD both profiles are implemented with ppp(8) and rfcomm_pppd(8) - a wrapper that converts RFCOMM Bluetooth connection into something PPP can operate with. Before any profile can be used, a new PPP label in the /etc/ppp/ppp.conf must be created. Consult rfcomm_pppd(8) manual page for examples.

In the following example rfcomm_pppd(8) will be used to open RFCOMM connection to remote device with BD_ADDR 00:80:37:29:19:a4 on DUN RFCOMM channel. The actual RFCOMM channel number will be obtained from the remote device via SDP. It is possible to specify RFCOMM channel by hand, and in this case rfcomm_pppd(8) will not perform SDP query. Use sdpcontrol(8) to find out RFCOMM channel on the remote device.

```
# rfcomm_pppd -a 00:80:37:29:19:a4 -c -C dun -l rfcomm-dialup
```

In order to provide Network Access with PPP (LAN) service the sdpd(8) server must be running. A new entry for LAN clients must be created in the /etc/ppp/ppp.conf file. Consult rfcomm_pppd(8) manual page for examples. Finally, start RFCOMM PPP server on valid RFCOMM channel number. The RFCOMM PPP server will automatically register Bluetooth LAN service with the local SDP daemon. The example below shows how to start RFCOMM PPP server.

```
# rfcomm_pppd -s -C 7 -l rfcomm-server
```

56.4.9. OBEX Object Push (OPUSH) Profile

OBEX is a widely used protocol for simple file transfers between mobile devices. Its main use is in infrared communication, where it is used for generic file transfers between notebooks or PDAs, and for sending business cards or calendar entries between cellular phones and other devices with PIM applications.

The OBEX server and client are implemented as a third-party package obexapp, which is available as comms/obexapp port.

OBEX client is used to push and/or pull objects from the OBEX server. An object can, for example, be a business card or an appointment. The OBEX client can obtain RFCOMM channel number from the remote device via SDP. This can be done by specifying service name instead of RFCOMM channel number. Supported service names are: IrMC, FTRN and OPUSH. It is possible to specify RFCOMM channel as a number. Below is an example of an OBEX session, where device information object is pulled from the cellular phone, and a new object (business card) is pushed into the phone's

directory.

```
% obexapp -a 00:80:37:29:19:a4 -C IrMC
obex> get telecom/devinfo.txt devinfo-t39.txt
Success, response: OK, Success (0x20)
obex> put new.vcf
Success, response: OK, Success (0x20)
obex> di
Success, response: OK, Success (0x20)
```

In order to provide OBEX Object Push service, sdpd(8) server must be running. A root folder, where all incoming objects will be stored, must be created. The default path to the root folder is /var/spool/obex. Finally, start OBEX server on valid RFCOMM channel number. The OBEX server will automatically register OBEX Object Push service with the local SDP daemon. The example below shows how to start OBEX server.

```
# obexapp -s -C 10
```

56.4.10. Serial Port Profile (SPP)

The Serial Port Profile (SPP) allows Bluetooth devices to perform RS232 (or similar) serial cable emulation. The scenario covered by this profile deals with legacy applications using Bluetooth as a cable replacement, through a virtual serial port abstraction.

The rfcomm_sppd(1) utility implements the Serial Port profile. A pseudo tty is used as a virtual serial port abstraction. The example below shows how to connect to a remote device Serial Port service. Note that you do not have to specify a RFCOMM channel - rfcomm_sppd(1) can obtain it from the remote device via SDP. If you would like to override this, specify a RFCOMM channel on the command line.

```
# rfcomm_sppd -a 00:07:E0:00:0B:CA -t /dev/ttyp6
rfcomm_sppd[94692]: Starting on /dev/ttyp6...
```

Once connected, the pseudo tty can be used as serial port:

```
# cu -l ttyp6
```

56.4.11. Troubleshooting

56.4.11.1. A remote device cannot connect

Some older Bluetooth devices do not support role switching. By default, when FreeBSD is accepting a new connection, it tries to perform a role switch and become master. Devices, which do not support this will not be able to connect. Note that role switching is performed when a new connection is being established, so it is not possible to ask the remote device if it does support role

switching. There is a HCI option to disable role switching on the local side:

```
# hccontrol -n ubt0hci write_node_role_switch 0
```

56.4.11.2. Something is going wrong, can I see what exactly is happening?

Yes, you can. Use the third-party package hcidump, which is available as comms/hcidump port. The hcidump utility is similar to tcpdump(1). It can be used to display the content of the Bluetooth packets on the terminal and to dump the Bluetooth packets to a file.

56.5. Bridging

56.5.1. Introduction

It is sometimes useful to divide one physical network (such as an Ethernet segment) into two separate network segments without having to create IP subnets and use a router to connect the segments together. A device that connects two networks together in this fashion is called a "bridge". A FreeBSD system with two network interface cards can act as a bridge.

The bridge works by learning the MAC layer addresses (Ethernet addresses) of the devices on each of its network interfaces. It forwards traffic between two networks only when its source and destination are on different networks.

In many respects, a bridge is like an Ethernet switch with very few ports.

56.5.2. Situations Where Bridging Is Appropriate

There are two common situations in which a bridge is used today.

56.5.2.1. High Traffic on a Segment

Situation one is where your physical network segment is overloaded with traffic, but you do not want for whatever reason to subnet the network and interconnect the subnets with a router.

Let us consider an example of a newspaper where the Editorial and Production departments are on the same subnetwork. The Editorial users all use server `A` for file service, and the Production users are on server `B`. An Ethernet network is used to connect all users together, and high loads on the network are slowing things down.

If the Editorial users could be segregated on one network segment and the Production users on another, the two network segments could be connected with a bridge. Only the network traffic destined for interfaces on the "other" side of the bridge would be sent to the other network, reducing congestion on each network segment.

56.5.2.2. Filtering/Traffic Shaping Firewall

The second common situation is where firewall functionality is needed without network address translation (NAT).

An example is a small company that is connected via DSL or ISDN to their ISP. They have a 13 globally-accessible IP addresses from their ISP and have 10 PCs on their network. In this situation, using a router-based firewall is difficult because of subnetting issues.

A bridge-based firewall can be configured and dropped into the path just downstream of their DSL/ISDN router without any IP numbering issues.

56.5.3. Configuring a Bridge

56.5.3.1. Network Interface Card Selection

A bridge requires at least two network cards to function. Unfortunately, not all network interface cards support bridging. Read bridge(4) for details on the cards that are supported.

Install and test the two network cards before continuing.

56.5.3.2. Kernel Configuration Changes

To enable kernel support for bridging, add the:

```
options BRIDGE
```

statement to your kernel configuration file, and rebuild your kernel.

56.5.3.3. Firewall Support

If you are planning to use the bridge as a firewall, you will need to add the `IPFIREWALL` option as well. Read Firewalls for general information on configuring the bridge as a firewall.

If you need to allow non-IP packets (such as ARP) to flow through the bridge, there are three options available. The first is to add the following option to the kernel and rebuild:

```
option  IPFIREWALL_DEFAULT_TO_ACCEPT
```

The second is to set the firewall type to “open” in the rc.conf file:

```
firewall_type="open"
```

Note that these options will make the firewall seem completely transparent; any packet or connection will be permitted by default. This may require significant changes to the firewall ruleset.

The third option is to apply the following ipfw(8) rule:

```
# ipfw add allow mac-type arp layer2
```

Or add it to the current firewall ruleset. This rule effectively allows arp(8) packets through, so it must be be applied near the beginning of the ruleset for early evaluation.

56.5.3.4. Traffic Shaping Support

If you want to use the bridge as a traffic shaper, you will need to add the DUMMYNET option to your kernel configuration. Read dummynet(4) for further information.

56.5.4. Enabling the Bridge

Add the line:

```
net.link.ether.bridge.enable=1
```

to /etc/sysctl.conf to enable the bridge at runtime, and the line:

```
net.link.ether.bridge.config=if1,if2
```

to enable bridging on the specified interfaces (replace *if1* and *if2* with the names of your two network interfaces). If you want the bridged packets to be filtered by ipfw(8), you should add:

```
net.link.ether.bridge.ipfw=1
```

as well.

For versions prior to FreeBSD 5.2-RELEASE, use instead the following lines:

```
net.link.ether.bridge=1
net.link.ether.bridge_cfg=if1,if2
net.link.ether.bridge_ipfw=1
```

56.5.5. Other Information

If you want to be able to ssh(1) into the bridge from the network, it is correct to assign one of the network cards an IP address. The consensus is that assigning both cards an address is a bad idea.

If you have multiple bridges on your network, there cannot be more than one path between any two workstations. Technically, this means that there is no support for spanning tree link management.

A bridge can add latency to your ping(8) times, especially for traffic from one segment to another.

56.6. Diskless Operation

A FreeBSD machine can boot over the network and operate without a local disk, using file systems

mounted from an NFS server. No system modification is necessary, beyond standard configuration files. Such a system is relatively easy to set up because all the necessary elements are readily available:

- There are at least two possible methods to load the kernel over the network:
  - PXE: The Intel® Preboot eXecution Environment system is a form of smart boot ROM built into some networking cards or motherboards. See pxeboot(8) for more details.
  - The Etherboot port (net/etherboot) produces ROM-able code to boot kernels over the network. The code can be either burnt into a boot PROM on a network card, or loaded from a local floppy (or hard) disk drive, or from a running MS-DOS® system. Many network cards are supported.
- A sample script (/usr/shared/examples/diskless/clone_root) eases the creation and maintenance of the workstation's root file system on the server. The script will probably require a little customization but it will get you started very quickly.
- Standard system startup files exist in /etc to detect and support a diskless system startup.
- Swapping, if needed, can be done either to an NFS file or to a local disk.

There are many ways to set up diskless workstations. Many elements are involved, and most can be customized to suit local taste. The following will describe variations on the setup of a complete system, emphasizing simplicity and compatibility with the standard FreeBSD startup scripts. The system described has the following characteristics:

- The diskless workstations use a shared read-only / file system, and a shared read-only /usr.

  The root file system is a copy of a standard FreeBSD root (typically the server's), with some configuration files overridden by ones specific to diskless operation or, possibly, to the workstation they belong to.

  The parts of the root which have to be writable are overlaid with md(4) file systems. Any changes will be lost when the system reboots.

- The kernel is transferred and loaded either with Etherboot or PXE as some situations may mandate the use of either method.

As described, this system is insecure. It should live in a protected area of a network, and be untrusted by other hosts.

All the information in this section has been tested using FreeBSD 5.2.1-RELEASE.

56.6.1. Background Information

Setting up diskless workstations is both relatively straightforward and prone to errors. These are sometimes difficult to diagnose for a number of reasons. For example:

- Compile time options may determine different behaviors at runtime.
- Error messages are often cryptic or totally absent.

In this context, having some knowledge of the background mechanisms involved is very useful to solve the problems that may arise.

Several operations need to be performed for a successful bootstrap:

- The machine needs to obtain initial parameters such as its IP address, executable filename, server name, root path. This is done using the DHCP or BOOTP protocols. DHCP is a compatible extension of BOOTP, and uses the same port numbers and basic packet format.

  It is possible to configure a system to use only BOOTP. The bootpd(8) server program is included in the base FreeBSD system.

  However, DHCP has a number of advantages over BOOTP (nicer configuration files, possibility of using PXE, plus many others not directly related to diskless operation), and we will describe mainly a DHCP configuration, with equivalent examples using bootpd(8) when possible. The sample configuration will use the ISC DHCP software package (release 3.0.1.r12 was installed on the test server).

- The machine needs to transfer one or several programs to local memory. Either TFTP or NFS are used. The choice between TFTP and NFS is a compile time option in several places. A common source of error is to specify filenames for the wrong protocol: TFTP typically transfers all files from a single directory on the server, and would expect filenames relative to this directory. NFS needs absolute file paths.
- The possible intermediate bootstrap programs and the kernel need to be initialized and executed. There are several important variations in this area:
  - PXE will load pxeboot(8), which is a modified version of the FreeBSD third stage loader. The loader(8) will obtain most parameters necessary to system startup, and leave them in the kernel environment before transferring control. It is possible to use a GENERIC kernel in this case.
  - Etherboot, will directly load the kernel, with less preparation. You will need to build a kernel with specific options.

    PXE and Etherboot work equally well; however, because kernels normally let the loader(8) do more work for them, PXE is the preferred method.

    If your BIOS and network cards support PXE, you should probably use it.
- Finally, the machine needs to access its file systems. NFS is used in all cases.

See also diskless(8) manual page.

56.6.2. Setup Instructions

56.6.2.1. Configuration Using ISC DHCP

The ISC DHCP server can answer both BOOTP and DHCP requests.

ISC DHCP 3.0 is not part of the base system. You will first need to install the net/isc-dhcp3-server port or the corresponding package.

Once ISC DHCP is installed, it needs a configuration file to run (normally named /usr/local/etc/dhcpd.conf). Here follows a commented example, where host `margaux` uses Etherboot and host `corbieres` uses PXE:

```
default-lease-time 600;
max-lease-time 7200;
authoritative;

option domain-name "example.com";
option domain-name-servers 192.168.4.1;
option routers 192.168.4.1;

subnet 192.168.4.0 netmask 255.255.255.0 {
  use-host-decl-names on; ①
  option subnet-mask 255.255.255.0;
  option broadcast-address 192.168.4.255;

  host margaux {
    hardware ethernet 01:23:45:67:89:ab;
    fixed-address margaux.example.com;
    next-server 192.168.4.4; ②
    filename "/data/misc/kernel.diskless"; ③
    option root-path "192.168.4.4:/data/misc/diskless"; ④
  }
  host corbieres {
    hardware ethernet 00:02:b3:27:62:df;
    fixed-address corbieres.example.com;
    next-server 192.168.4.4;
    filename "pxeboot";
    option root-path "192.168.4.4:/data/misc/diskless";
  }
}
```

① This option tells dhcpd to send the value in the `host` declarations as the hostname for the diskless host. An alternate way would be to add an `option host-name margaux` inside the `host` declarations.

② The `next-server` directive designates the TFTP or NFS server to use for loading loader or kernel file (the default is to use the same host as the DHCP server).

③ The `filename` directive defines the file that Etherboot or PXE will load for the next execution step. It must be specified according to the transfer method used. Etherboot can be compiled to use NFS or TFTP. The FreeBSD port configures NFS by default. PXE uses TFTP, which is why a relative filename is used here (this may depend on the TFTP server configuration, but would be fairly typical). Also, PXE loads pxeboot, not the kernel. There are other interesting possibilities, like loading pxeboot from a FreeBSD CD-ROM /boot directory (as pxeboot(8) can load a GENERIC kernel, this makes it possible to use PXE to boot from a remote CD-ROM).

④ The `root-path` option defines the path to the root file system, in usual NFS notation. When using PXE, it is possible to leave off the host's IP as long as you do not enable the kernel option BOOTP. The NFS server will then be the same as the TFTP one.

56.6.2.2. Configuration Using BOOTP

Here follows an equivalent bootpd configuration (reduced to one client). This would be found in /etc/bootptab.

Please note that Etherboot must be compiled with the non-default option `NO_DHCP_SUPPORT` in order to use BOOTP, and that PXE_needs_DHCP. The only obvious advantage of bootpd is that it exists in the base system.

```
.def100:\
  :hn:ht=1:sa=192.168.4.4:vm=rfc1048:\
  :sm=255.255.255.0:\
  :ds=192.168.4.1:\
  :gw=192.168.4.1:\
  :hd="/tftpboot":\
  :bf="/kernel.diskless":\
  :rp="192.168.4.4:/data/misc/diskless":

margaux:ha=0123456789ab:tc=.def100
```

56.6.2.3. Preparing a Boot Program with Etherboot

Etherboot's Web site contains extensive documentation mainly intended for Linux systems, but nonetheless containing useful information. The following will just outline how you would use Etherboot on a FreeBSD system.

You must first install the net/etherboot package or port.

You can change the Etherboot configuration (i.e. to use TFTP instead of NFS) by editing the Config file in the Etherboot source directory.

For our setup, we shall use a boot floppy. For other methods (PROM, or MS-DOS® program), please refer to the Etherboot documentation.

To make a boot floppy, insert a floppy in the drive on the machine where you installed Etherboot, then change your current directory to the src directory in the Etherboot tree and type:

```
# gmake bin32/devicetype.fd0
```

devicetype depends on the type of the Ethernet card in the diskless workstation. Refer to the NIC file in the same directory to determine the right *devicetype*.

56.6.2.4. Booting with PXE

By default, the pxeboot(8) loader loads the kernel via NFS. It can be compiled to use TFTP instead by specifying the `LOADER_TFTP_SUPPORT` option in /etc/make.conf. See the comments in /usr/shared/examples/etc/make.conf for instructions.

There are two other make.conf options which may be useful for setting up a serial console diskless

machine: BOOT_PXELDR_PROBE_KEYBOARD, and BOOT_PXELDR_ALWAYS_SERIAL.

To use PXE when the machine starts, you will usually need to select the Boot from network option in your BIOS setup, or type a function key during the PC initialization.

56.6.2.5. Configuring the TFTP and NFS Servers

If you are using PXE or Etherboot configured to use TFTP, you need to enable tftpd on the file server:

1. Create a directory from which tftpd will serve the files, e.g. /tftpboot.
2. Add this line to your /etc/inetd.conf:

```
tftp    dgram   udp wait    root    /usr/libexec/tftpd  tftpd -l -s /tftpboot
```

It appears that at least some PXE versions want the TCP version of TFTP. In this case, add a second line, replacing dgram udp with stream tcp.

3. Tell inetd to reread its configuration file. The inetd_enable="YES" must be in the /etc/rc.conf file for this command to execute correctly:

```
# /etc/rc.d/inetd restart
```

You can place the tftpboot directory anywhere on the server. Make sure that the location is set in both inetd.conf and dhcpd.conf.

In all cases, you also need to enable NFS and export the appropriate file system on the NFS server.

1. Add this to /etc/rc.conf:

```
nfs_server_enable="YES"
```

2. Export the file system where the diskless root directory is located by adding the following to /etc/exports (adjust the volume mount point and replace *margaux corbieres* with the names of the diskless workstations):

```
/data/misc -alldirs -ro margaux corbieres
```

3. Tell mountd to reread its configuration file. If you actually needed to enable NFS in /etc/rc.conf at the first step, you probably want to reboot instead.

```
# /etc/rc.d/mountd restart
```

56.6.2.6. Building a Diskless Kernel

If using Etherboot, you need to create a kernel configuration file for the diskless client with the following options (in addition to the usual ones):

```
options     BOOTP          # Use BOOTP to obtain IP address/hostname
options     BOOTP_NFSROOT  # NFS mount root file system using BOOTP info
```

You may also want to use `BOOTP_NFSV3`, `BOOT_COMPAT` and `BOOTP_WIRED_TO` (refer to NOTES).

These option names are historical and slightly misleading as they actually enable indifferent use of DHCP and BOOTP inside the kernel (it is also possible to force strict BOOTP or DHCP use).

Build the kernel (see Ρυθμίζοντας τον Πυρήνα του FreeBSD), and copy it to the place specified in dhcpd.conf.

When using PXE, building a kernel with the above options is not strictly necessary (though suggested). Enabling them will cause more DHCP requests to be issued during kernel startup, with a small risk of inconsistency between the new values and those retrieved by pxeboot(8) in some special cases. The advantage of using them is that the host name will be set as a side effect. Otherwise you will need to set the host name by another method, for example in a client-specific rc.conf file.

In order to be loadable with Etherboot, a kernel needs to have the device hints compiled in. You would typically set the following option in the configuration file (see the NOTES configuration comments file):

```
hints       "GENERIC.hints"
```

56.6.2.7. Preparing the Root Filesystem

You need to create a root file system for the diskless workstations, in the location listed as `root-path` in dhcpd.conf.

56.6.2.7.1. Using `make world` to populate root

This method is quick and will install a complete virgin system (not only the root file system) into `DESTDIR`. All you have to do is simply execute the following script:

```
#!/bin/sh
export DESTDIR=/data/misc/diskless
mkdir -p ${DESTDIR}
cd /usr/src; make buildworld && make buildkernel
cd /usr/src/etc; make distribution
```

Once done, you may need to customize your /etc/rc.conf and /etc/fstab placed into `DESTDIR` according

to your needs.

56.6.2.8. Configuring Swap

If needed, a swap file located on the server can be accessed via NFS.

56.6.2.8.1. NFS Swap

The kernel does not support enabling NFS swap at boot time. Swap must be enabled by the startup scripts, by mounting a writable file system and creating and enabling a swap file. To create a swap file of appropriate size, you can do like this:

```
# dd if=/dev/zero of=/path/to/swapfile bs=1k count=1 oseek=100000
```

To enable it you have to add the following line to your rc.conf:

```
swapfile=/path/to/swapfile
```

56.6.2.9. Miscellaneous Issues

56.6.2.9.1. Running with a Read-only /usr

If the diskless workstation is configured to run X, you will have to adjust the XDM configuration file, which puts the error log on /usr by default.

56.6.2.9.2. Using a Non-FreeBSD Server

When the server for the root file system is not running FreeBSD, you will have to create the root file system on a FreeBSD machine, then copy it to its destination, using `tar` or `cpio`.

In this situation, there are sometimes problems with the special files in /dev, due to differing major/minor integer sizes. A solution to this problem is to export a directory from the non-FreeBSD server, mount this directory onto a FreeBSD machine, and use devfs(5) to allocate device nodes transparently for the user.

56.7. ISDN

A good resource for information on ISDN technology and hardware is Dan Kegel's ISDN Page.

A quick simple road map to ISDN follows:

- If you live in Europe you might want to investigate the ISDN card section.
- If you are planning to use ISDN primarily to connect to the Internet with an Internet Provider on a dial-up non-dedicated basis, you might look into Terminal Adapters. This will give you the most flexibility, with the fewest problems, if you change providers.
- If you are connecting two LANs together, or connecting to the Internet with a dedicated ISDN connection, you might consider the stand alone router/bridge option.

Cost is a significant factor in determining what solution you will choose. The following options are listed from least expensive to most expensive.

56.7.1. ISDN Cards

FreeBSD's ISDN implementation supports only the DSS1/Q.931 (or Euro-ISDN) standard using passive cards. Some active cards are supported where the firmware also supports other signaling protocols; this also includes the first supported Primary Rate (PRI) ISDN card.

The isdn4bsd software allows you to connect to other ISDN routers using either IP over raw HDLC or by using synchronous PPP: either by using kernel PPP with `isppp`, a modified sppp(4) driver, or by using userland ppp(8). By using userland ppp(8), channel bonding of two or more ISDN B-channels is possible. A telephone answering machine application is also available as well as many utilities such as a software 300 Baud modem.

Some growing number of PC ISDN cards are supported under FreeBSD and the reports show that it is successfully used all over Europe and in many other parts of the world.

The passive ISDN cards supported are mostly the ones with the Infineon (formerly Siemens) ISAC/HSCX/IPAC ISDN chipsets, but also ISDN cards with chips from Cologne Chip (ISA bus only), PCI cards with Winbond W6692 chips, some cards with the Tiger300/320/ISAC chipset combinations and some vendor specific chipset based cards such as the AVM Fritz!Card PCI V.1.0 and the AVM Fritz!Card PnP.

Currently the active supported ISDN cards are the AVM B1 (ISA and PCI) BRI cards and the AVM T1 PCI PRI cards.

For documentation on isdn4bsd, have a look at /usr/shared/examples/isdn/ directory on your FreeBSD system or at the homepage of isdn4bsd which also has pointers to hints, erratas and much more documentation such as the isdn4bsd handbook.

In case you are interested in adding support for a different ISDN protocol, a currently unsupported ISDN PC card or otherwise enhancing isdn4bsd, please get in touch with Hellmuth Michaelis <hm@FreeBSD.org>.

For questions regarding the installation, configuration and troubleshooting isdn4bsd, a freebsd-isdn mailing list is available.

56.7.2. ISDN Terminal Adapters

Terminal adapters (TA), are to ISDN what modems are to regular phone lines.

Most TA's use the standard Hayes modem AT command set, and can be used as a drop in replacement for a modem.

A TA will operate basically the same as a modem except connection and throughput speeds will be much faster than your old modem. You will need to configure PPP exactly the same as for a modem setup. Make sure you set your serial speed as high as possible.

The main advantage of using a TA to connect to an Internet Provider is that you can do Dynamic

PPP. As IP address space becomes more and more scarce, most providers are not willing to provide you with a static IP anymore. Most stand-alone routers are not able to accommodate dynamic IP allocation.

TA's completely rely on the PPP daemon that you are running for their features and stability of connection. This allows you to upgrade easily from using a modem to ISDN on a FreeBSD machine, if you already have PPP set up. However, at the same time any problems you experienced with the PPP program and are going to persist.

If you want maximum stability, use the kernel PPP option, not the userland PPP.

The following TA's are known to work with FreeBSD:

- Motorola BitSurfer and Bitsurfer Pro
- Adtran

Most other TA's will probably work as well, TA vendors try to make sure their product can accept most of the standard modem AT command set.

The real problem with external TA's is that, like modems, you need a good serial card in your computer.

You should read the FreeBSD Serial Hardware tutorial for a detailed understanding of serial devices, and the differences between asynchronous and synchronous serial ports.

A TA running off a standard PC serial port (asynchronous) limits you to 115.2 Kbs, even though you have a 128 Kbs connection. To fully utilize the 128 Kbs that ISDN is capable of, you must move the TA to a synchronous serial card.

Do not be fooled into buying an internal TA and thinking you have avoided the synchronous/asynchronous issue. Internal TA's simply have a standard PC serial port chip built into them. All this will do is save you having to buy another serial cable and find another empty electrical socket.

A synchronous card with a TA is at least as fast as a stand-alone router, and with a simple 386 FreeBSD box driving it, probably more flexible.

The choice of synchronous card/TA v.s. stand-alone router is largely a religious issue. There has been some discussion of this in the mailing lists. We suggest you search the archives for the complete discussion.

56.7.3. Stand-alone ISDN Bridges/Routers

ISDN bridges or routers are not at all specific to FreeBSD or any other operating system. For a more complete description of routing and bridging technology, please refer to a networking reference book.

In the context of this section, the terms router and bridge will be used interchangeably.

As the cost of low end ISDN routers/bridges comes down, it will likely become a more and more

popular choice. An ISDN router is a small box that plugs directly into your local Ethernet network, and manages its own connection to the other bridge/router. It has built in software to communicate via PPP and other popular protocols.

A router will allow you much faster throughput than a standard TA, since it will be using a full synchronous ISDN connection.

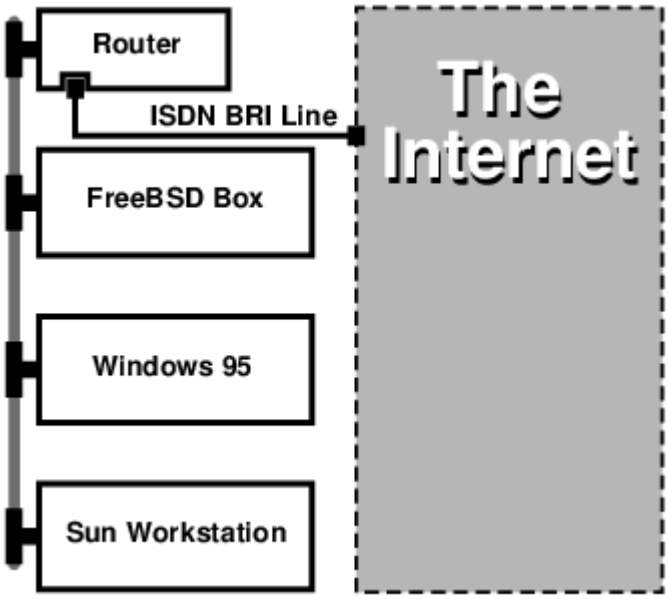
The main problem with ISDN routers and bridges is that interoperability between manufacturers can still be a problem. If you are planning to connect to an Internet provider, you should discuss your needs with them.

If you are planning to connect two LAN segments together, such as your home LAN to the office LAN, this is the simplest lowest maintenance solution. Since you are buying the equipment for both sides of the connection you can be assured that the link will work.

For example to connect a home computer or branch office network to a head office network the following setup could be used:

Παράδειγμα 26. Branch Office or Home Network

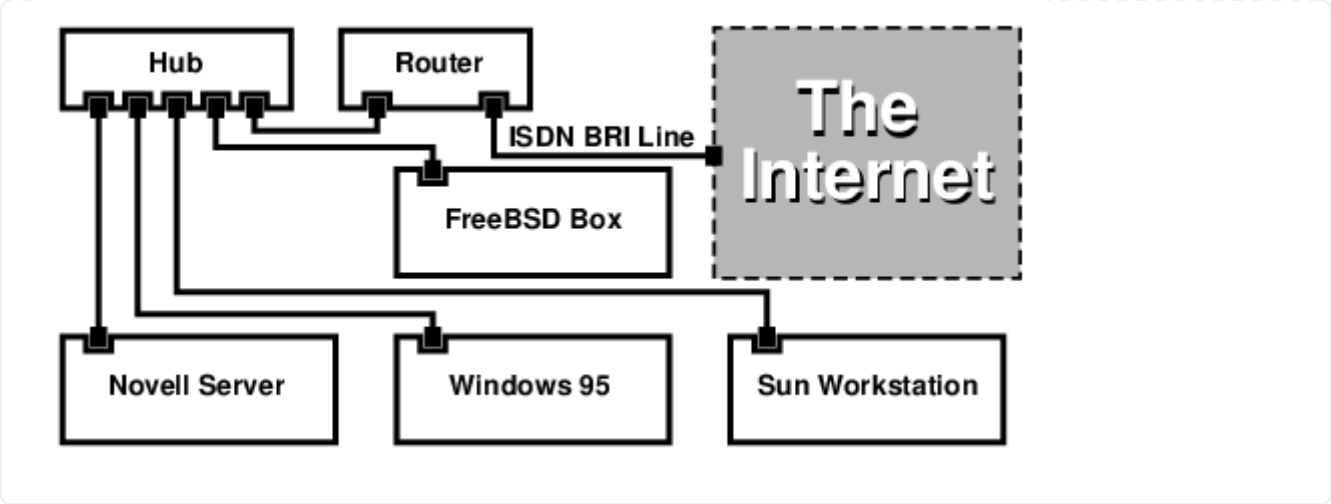
Network uses a bus based topology with 10 base 2 Ethernet ("thinnet"). Connect router to network cable with AUI/10BT transceiver, if necessary.



If your home/branch office is only one computer you can use a twisted pair crossover cable to connect to the stand-alone router directly.

Παράδειγμα 27. Head Office or Other LAN

Network uses a star topology with 10 base T Ethernet ("Twisted Pair").



One large advantage of most routers/bridges is that they allow you to have 2 *separate independent* PPP connections to 2 separate sites at the *same* time. This is not supported on most TA's, except for specific (usually expensive) models that have two serial ports. Do not confuse this with channel bonding, MPP, etc.

This can be a very useful feature if, for example, you have an dedicated ISDN connection at your office and would like to tap into it, but do not want to get another ISDN line at work. A router at the office location can manage a dedicated B channel connection (64 Kbps) to the Internet and use the other B channel for a separate data connection. The second B channel can be used for dial-in, dial-out or dynamically bonding (MPP, etc.) with the first B channel for more bandwidth.

An Ethernet bridge will also allow you to transmit more than just IP traffic. You can also send IPX/SPX or whatever other protocols you use.

56.8. Network Address Translation

56.8.1. Overview

FreeBSD's Network Address Translation daemon, commonly known as natd(8) is a daemon that accepts incoming raw IP packets, changes the source to the local machine and re-injects these packets back into the outgoing IP packet stream. natd(8) does this by changing the source IP address and port such that when data is received back, it is able to determine the original location of the data and forward it back to its original requester.

The most common use of NAT is to perform what is commonly known as Internet Connection Sharing.

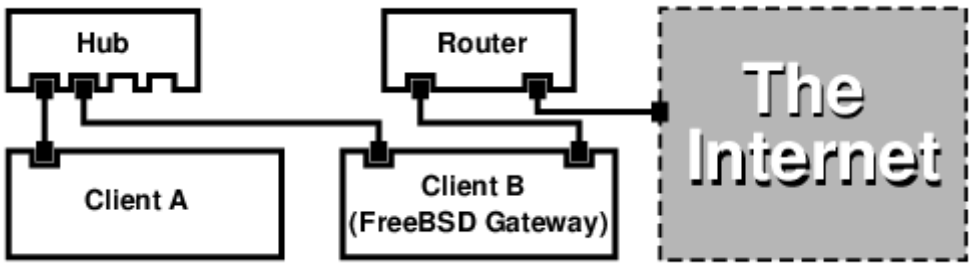
56.8.2. Setup

Due to the diminishing IP space in IPv4, and the increased number of users on high-speed consumer lines such as cable or DSL, people are increasingly in need of an Internet Connection Sharing solution. The ability to connect several computers online through one connection and IP address makes natd(8) a reasonable choice.

Most commonly, a user has a machine connected to a cable or DSL line with one IP address and wishes to use this one connected computer to provide Internet access to several more over a LAN.

To do this, the FreeBSD machine on the Internet must act as a gateway. This gateway machine must have two NICs-one for connecting to the Internet router, the other connecting to a LAN. All the machines on the LAN are connected through a hub or switch.

There are many ways to get a LAN connected to the Internet through a FreeBSD gateway. This example will only cover a gateway with at least two NICs.



A setup like this is commonly used to share an Internet connection. One of the LAN machines is connected to the Internet. The rest of the machines access the Internet through that "gateway" machine.

56.8.3. Configuration

The following options must be in the kernel configuration file:

```
options IPFIREWALL
options IPDIVERT
```

Additionally, at choice, the following may also be suitable:

```
options IPFIREWALL_DEFAULT_TO_ACCEPT
options IPFIREWALL_VERBOSE
```

The following must be in /etc/rc.conf:

```
gateway_enable="YES" ①
firewall_enable="YES" ②
firewall_type="OPEN" ③
natd_enable="YES"
natd_interface="fxp0" ④
natd_flags="" ⑤
```

① Sets up the machine to act as a gateway. Running `sysctl net.inet.ip.forwarding=1` would have the same effect.

② Enables the firewall rules in /etc/rc.firewall at boot.

③ This specifies a predefined firewall ruleset that allows anything in. See /etc/rc.firewall for additional types.

④ Indicates which interface to forward packets through (the interface connected to the Internet).

⑤ Any additional configuration options passed to natd(8) on boot.

Having the previous options defined in /etc/rc.conf would run `natd -interface fxp0` at boot. This can also be run manually.

It is also possible to use a configuration file for natd(8) when there are too many options to pass. In this case, the configuration file must be defined by adding the following line to /etc/rc.conf:

```
natd_flags="-f /etc/natd.conf"
```

The /etc/natd.conf file will contain a list of configuration options, one per line. For example the next section case would use the following file:

```
redirect_port tcp 192.168.0.2:6667 6667
redirect_port tcp 192.168.0.3:80 80
```

For more information about the configuration file, consult the natd(8) manual page about the `-f` option.

Each machine and interface behind the LAN should be assigned IP address numbers in the private network space as defined by RFC 1918 and have a default gateway of the natd machine's internal IP address.

For example, client `A` and `B` behind the LAN have IP addresses of `192.168.0.2` and `192.168.0.3`, while the natd machine's LAN interface has an IP address of `192.168.0.1`. Client `A` and `B`'s default gateway must be set to that of the natd machine, `192.168.0.1`. The natd machine's external, or Internet interface does not require any special modification for natd(8) to work.

56.8.4. Port Redirection

The drawback with natd(8) is that the LAN clients are not accessible from the Internet. Clients on the LAN can make outgoing connections to the world but cannot receive incoming ones. This presents a problem if trying to run Internet services on one of the LAN client machines. A simple way around this is to redirect selected Internet ports on the natd machine to a LAN client.

For example, an IRC server runs on client `A`, and a web server runs on client `B`. For this to work properly, connections received on ports 6667 (IRC) and 80 (web) must be redirected to the respective machines.

The `-redirect_port` must be passed to natd(8) with the proper options. The syntax is as follows:

```
    -redirect_port proto targetIP:targetPORT[-targetPORT]
                [aliasIP:]aliasPORT[-aliasPORT]
                [remoteIP[:remotePORT[-remotePORT]]]
```

In the above example, the argument should be:

```
    -redirect_port tcp 192.168.0.2:6667 6667
    -redirect_port tcp 192.168.0.3:80 80
```

```
This will redirect the proper _tcp_ ports to the LAN client machines.
```

The `-redirect_port` argument can be used to indicate port ranges over individual ports. For example, *tcp 192.168.0.2:2000-3000 2000-3000* would redirect all connections received on ports 2000 to 3000 to ports 2000 to 3000 on client `A`.

These options can be used when directly running natd(8), placed within the `natd_flags=""` option in /etc/rc.conf, or passed via a configuration file.

For further configuration options, consult natd(8)

56.8.5. Address Redirection

Address redirection is useful if several IP addresses are available, yet they must be on one machine. With this, natd(8) can assign each LAN client its own external IP address. natd(8) then rewrites outgoing packets from the LAN clients with the proper external IP address and redirects all traffic incoming on that particular IP address back to the specific LAN client. This is also known as static NAT. For example, the IP addresses `128.1.1.1`, `128.1.1.2`, and `128.1.1.3` belong to the natd gateway machine. `128.1.1.1` can be used as the natd gateway machine's external IP address, while `128.1.1.2` and `128.1.1.3` are forwarded back to LAN clients `A` and `B`.

The `-redirect_address` syntax is as follows:

```
-redirect_address localIP publicIP
```

localIP	The internal IP address of the LAN client.
publicIP	The external IP address corresponding to the LAN client.

In the example, this argument would read:

```
-redirect_address 192.168.0.2 128.1.1.2
-redirect_address 192.168.0.3 128.1.1.3
```

Like `-redirect_port`, these arguments are also placed within the `natd_flags=""` option of /etc/rc.conf, or passed via a configuration file. With address redirection, there is no need for port redirection since all data received on a particular IP address is redirected.

The external IP addresses on the natd machine must be active and aliased to the external interface. Look at rc.conf(5) to do so.

56.9. Parallel Line IP (PLIP)

PLIP lets us run TCP/IP between parallel ports. It is useful on machines without network cards, or to install on laptops. In this section, we will discuss:

- Creating a parallel (laplink) cable.
- Connecting two computers with PLIP.

56.9.1. Creating a Parallel Cable

You can purchase a parallel cable at most computer supply stores. If you cannot do that, or you just want to know how it is done, the following table shows how to make one out of a normal parallel printer cable.

Πίνακας 8. Wiring a Parallel Cable for Networking

A-name	A-End	B-End	Descr.	Post/Bit
.... DATA0 -ERROR	.... 2 15	.... 15 2	Data	.... 0/0x01 1/0x08 ....
.... DATA1 +SLCT	.... 3 13	.... 13 3	Data	.... 0/0x02 1/0x10 ....
.... DATA2 +PE	.... 4 12	.... 12 4	Data	.... 0/0x04 1/0x20 ....
.... DATA3 -ACK	.... 5 10	.... 10 5	Strobe	.... 0/0x08 1/0x40 ....
.... DATA4 BUSY	.... 6 11	.... 11 6	Data	.... 0/0x10 1/0x80 ....
GND	18-25	18-25	GND	-

56.9.2. Setting Up PLIP

First, you have to get a laplink cable. Then, confirm that both computers have a kernel with lpt(4) driver support:

```
# grep lp /var/run/dmesg.boot
lpt0: <Printer> on ppbus0
```

```
lpt0: Interrupt-driven port
```

The parallel port must be an interrupt driven port, you should have lines similar to the following in your in the /boot/device.hints file:

```
hint.ppc.0.at="isa"
hint.ppc.0.irq="7"
```

Then check if the kernel configuration file has a `device plip` line or if the plip.ko kernel module is loaded. In both cases the parallel networking interface should appear when you use the ifconfig(8) command to display it:

```
# ifconfig plip0
plip0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
```

Plug the laplink cable into the parallel interface on both computers.

Configure the network interface parameters on both sites as `root`. For example, if you want to connect the host `host1` with another machine `host2`:

```
                host1 <-----> host2
IP Address    10.0.0.1      10.0.0.2
```

Configure the interface on `host1` by doing:

```
# ifconfig plip0 10.0.0.1 10.0.0.2
```

Configure the interface on `host2` by doing:

```
# ifconfig plip0 10.0.0.2 10.0.0.1
```

You now should have a working connection. Please read the manual pages lp(4) and lpt(4) for more details.

You should also add both hosts to /etc/hosts:

```
127.0.0.1               localhost.my.domain localhost
10.0.0.1                host1.my.domain host1
10.0.0.2                host2.my.domain
```

To confirm the connection works, go to each host and ping the other. For example, on `host1`:

```
# ifconfig plip0
```

```
plip0: flags=8851<UP,POINTOPOINT,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 10.0.0.1 --> 10.0.0.2 netmask 0xff000000
# netstat -r
Routing tables

Internet:
Destination        Gateway           Flags     Refs     Use      Netif Expire
host2              host1             UH          0       0       plip0
# ping -c 4 host2
PING host2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=255 time=2.774 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=255 time=2.530 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=255 time=2.556 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=255 time=2.714 ms

--- host2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 2.530/2.643/2.774/0.103 ms
```

56.10. IPv6

IPv6 (also known as IPng "IP next generation") is the new version of the well known IP protocol (also known as IPv4). Like the other current *BSD systems, FreeBSD includes the KAME IPv6 reference implementation. So your FreeBSD system comes with all you will need to experiment with IPv6. This section focuses on getting IPv6 configured and running.

In the early 1990s, people became aware of the rapidly diminishing address space of IPv4. Given the expansion rate of the Internet there were two major concerns:

- Running out of addresses. Today this is not so much of a concern anymore since RFC1918 private address space (`10.0.0.0/8`, `172.16.0.0/12`, and `192.168.0.0/16`) and Network Address Translation (NAT) are being employed.
- Router table entries were getting too large. This is still a concern today.

IPv6 deals with these and many other issues:

- 128 bit address space. In other words theoretically there are 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses available. This means there are approximately 6.67 * 10^27 IPv6 addresses per square meter on our planet.
- Routers will only store network aggregation addresses in their routing tables thus reducing the average space of a routing table to 8192 entries.

There are also lots of other useful features of IPv6 such as:

- Address autoconfiguration (RFC2462)
- Anycast addresses ("one-out-of many")
- Mandatory multicast addresses

- IPsec (IP security)
- Simplified header structure
- Mobile IP
- IPv6-to-IPv4 transition mechanisms

For more information see:

- IPv6 overview at playground.sun.com
- KAME.net

56.10.1. Background on IPv6 Addresses

There are different types of IPv6 addresses: Unicast, Anycast and Multicast.

Unicast addresses are the well known addresses. A packet sent to a unicast address arrives exactly at the interface belonging to the address.

Anycast addresses are syntactically indistinguishable from unicast addresses but they address a group of interfaces. The packet destined for an anycast address will arrive at the nearest (in router metric) interface. Anycast addresses may only be used by routers.

Multicast addresses identify a group of interfaces. A packet destined for a multicast address will arrive at all interfaces belonging to the multicast group.

The IPv4 broadcast address (usually `xxx.xxx.xxx.255`) is expressed by multicast addresses in IPv6.

Πίνακας 9. Reserved IPv6 addresses

IPv6 address	Prefixlength (Bits)	Description	Notes
`::`	128 bits	unspecified	cf. `0.0.0.0` in IPv4
`::1`	128 bits	loopback address	cf. `127.0.0.1` in IPv4
`::00:xx:xx:xx:xx`	96 bits	embedded IPv4	The lower 32 bits are the IPv4 address. Also called "IPv4 compatible IPv6 address"
`::ff:xx:xx:xx:xx`	96 bits	IPv4 mapped IPv6 address	The lower 32 bits are the IPv4 address. For hosts which do not support IPv6.
`fe80::` - `feb::`	10 bits	link-local	cf. loopback address in IPv4
`fec0::` - `fef::`	10 bits	site-local	
`ff::`	8 bits	multicast	

IPv6 address	Prefixlength (Bits)	Description	Notes
001 (base 2)	3 bits	global unicast	All global unicast addresses are assigned from this pool. The first 3 bits are "001".

56.10.2. Reading IPv6 Addresses

The canonical form is represented as: x:x:x:x:x:x:x:x, each "x" being a 16 Bit hex value. For example FEBC:A574:382B:23C1:AA49:4592:4EFE:9982

Often an address will have long substrings of all zeros therefore one such substring per address can be abbreviated by "::". Also up to three leading "0"s per hexquad can be omitted. For example fe80::1 corresponds to the canonical form fe80:0000:0000:0000:0000:0000:0000:0001.

A third form is to write the last 32 Bit part in the well known (decimal) IPv4 style with dots "." as separators. For example 2002::10.0.0.1 corresponds to the (hexadecimal) canonical representation 2002:0000:0000:0000:0000:0000:0a00:0001 which in turn is equivalent to writing 2002::a00:1.

By now the reader should be able to understand the following:

```
# ifconfig
```

```
rl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
         inet 10.0.0.10 netmask 0xffffff00 broadcast 10.0.0.255
         inet6 fe80::200:21ff:fe03:8e1%rl0 prefixlen 64 scopeid 0x1
         ether 00:00:21:03:08:e1
         media: Ethernet autoselect (100baseTX )
         status: active
```

fe80::200:21ff:fe03:8e1%rl0 is an auto configured link-local address. It is generated from the MAC address as part of the auto configuration.

For further information on the structure of IPv6 addresses see RFC3513.

56.10.3. Getting Connected

Currently there are four ways to connect to other IPv6 hosts and networks:

- Getting an IPv6 network from your upstream provider. Talk to your Internet provider for instructions.
- Tunnel via 6-to-4 (RFC3068)
- Use the net/freenet6 port if you are on a dial-up connection.

56.10.4. DNS in the IPv6 World

There used to be two types of DNS records for IPv6. The IETF has declared A6 records obsolete. AAAA records are the standard now.

Using AAAA records is straightforward. Assign your hostname to the new IPv6 address you just received by adding:

```
MYHOSTNAME           AAAA    MYIPv6ADDR
```

To your primary zone DNS file. In case you do not serve your own DNS zones ask your DNS provider. Current versions of bind (version 8.3 and 9) and dns/djbdns (with the IPv6 patch) support AAAA records.

56.10.5. Applying the needed changes to /etc/rc.conf

56.10.5.1. IPv6 Client Settings

These settings will help you configure a machine that will be on your LAN and act as a client, not a router. To have rtsol(8) autoconfigure your interface on boot all you need to add is:

```
ipv6_enable="YES"
```

To statically assign an IP address such as `2001:471:1f11:251:290:27ff:fee0:2093`, to your fxp0 interface, add:

```
ipv6_ifconfig_fxp0="2001:471:1f11:251:290:27ff:fee0:2093"
```

To assign a default router of `2001:471:1f11:251::1` add the following to /etc/rc.conf:

```
ipv6_defaultrouter="2001:471:1f11:251::1"
```

56.10.5.2. IPv6 Router/Gateway Settings

This will help you take the directions that your tunnel provider has given you and convert it into settings that will persist through reboots. To restore your tunnel on startup use something like the following in /etc/rc.conf:

List the Generic Tunneling interfaces that will be configured, for example gif0:

```
gif_interfaces="gif0"
```

To configure the interface with a local endpoint of *MY_IPv4_ADDR* to a remote endpoint of *REMOTE_IPv4_ADDR*:

```
gifconfig_gif0="MY_IPv4_ADDR REMOTE_IPv4_ADDR"
```

To apply the IPv6 address you have been assigned for use as your IPv6 tunnel endpoint, add:

```
ipv6_ifconfig_gif0="MY_ASSIGNED_IPv6_TUNNEL_ENDPOINT_ADDR"
```

Then all you have to do is set the default route for IPv6. This is the other side of the IPv6 tunnel:

```
ipv6_defaultrouter="MY_IPv6_REMOTE_TUNNEL_ENDPOINT_ADDR"
```

56.10.5.3. IPv6 Tunnel Settings

If the server is to route IPv6 between the rest of your network and the world, the following /etc/rc.conf setting will also be needed:

```
ipv6_gateway_enable="YES"
```

56.10.6. Router Advertisement and Host Auto Configuration

This section will help you setup rtadvd(8) to advertise the IPv6 default route.

To enable rtadvd(8) you will need the following in your /etc/rc.conf:

```
rtadvd_enable="YES"
```

It is important that you specify the interface on which to do IPv6 router solicitation. For example to tell rtadvd(8) to use fxp0:

```
rtadvd_interfaces="fxp0"
```

Now we must create the configuration file, /etc/rtadvd.conf. Here is an example:

```
fxp0:\
    :addrs#1:addr="2001:471:1f11:246::":prefixlen#64:tc=ether:
```

Replace fxp0 with the interface you are going to be using.

Next, replace `2001:471:1f11:246::` with the prefix of your allocation.

If you are dedicated a `/64` subnet you will not need to change anything else. Otherwise, you will need to change the `prefixlen#` to the correct value.

56.11. Asynchronous Transfer Mode (ATM)

56.11.1. Configuring classical IP over ATM (PVCs)

Classical IP over ATM (CLIP) is the simplest method to use Asynchronous Transfer Mode (ATM) with IP. It can be used with switched connections (SVCs) and with permanent connections (PVCs). This section describes how to set up a network based on PVCs.

56.11.1.1. Fully meshed configurations

The first method to set up a CLIP with PVCs is to connect each machine to each other machine in the network via a dedicated PVC. While this is simple to configure it tends to become impractical for a larger number of machines. The example supposes that we have four machines in the network, each connected to the ATM network with an ATM adapter card. The first step is the planning of the IP addresses and the ATM connections between the machines. We use the following:

Host	IP Address
hostA	192.168.173.1
hostB	192.168.173.2
hostC	192.168.173.3
hostD	192.168.173.4

To build a fully meshed net we need one ATM connection between each pair of machines:

Machines	VPI.VCI couple
hostA - hostB	0.100
hostA - hostC	0.101
hostA - hostD	0.102
hostB - hostC	0.103
hostB - hostD	0.104
hostC - hostD	0.105

The VPI and VCI values at each end of the connection may of course differ, but for simplicity we assume that they are the same. Next we need to configure the ATM interfaces on each host:

```
hostA# ifconfig hatm0 192.168.173.1 up
hostB# ifconfig hatm0 192.168.173.2 up
hostC# ifconfig hatm0 192.168.173.3 up
hostD# ifconfig hatm0 192.168.173.4 up
```

assuming that the ATM interface is hatm0 on all hosts. Now the PVCs need to be configured on hostA (we assume that they are already configured on the ATM switches, you need to consult the manual for the switch on how to do this).

```
hostA# atmconfig natm add 192.168.173.2 hatm0 0 100 llc/snap ubr
hostA# atmconfig natm add 192.168.173.3 hatm0 0 101 llc/snap ubr
hostA# atmconfig natm add 192.168.173.4 hatm0 0 102 llc/snap ubr

hostB# atmconfig natm add 192.168.173.1 hatm0 0 100 llc/snap ubr
hostB# atmconfig natm add 192.168.173.3 hatm0 0 103 llc/snap ubr
hostB# atmconfig natm add 192.168.173.4 hatm0 0 104 llc/snap ubr

hostC# atmconfig natm add 192.168.173.1 hatm0 0 101 llc/snap ubr
hostC# atmconfig natm add 192.168.173.2 hatm0 0 103 llc/snap ubr
hostC# atmconfig natm add 192.168.173.4 hatm0 0 105 llc/snap ubr

hostD# atmconfig natm add 192.168.173.1 hatm0 0 102 llc/snap ubr
hostD# atmconfig natm add 192.168.173.2 hatm0 0 104 llc/snap ubr
hostD# atmconfig natm add 192.168.173.3 hatm0 0 105 llc/snap ubr
```

Of course other traffic contracts than UBR can be used given the ATM adapter supports those. In this case the name of the traffic contract is followed by the parameters of the traffic. Help for the atmconfig(8) tool can be obtained with:

```
# atmconfig help natm add
```

or in the atmconfig(8) manual page.

The same configuration can also be done via /etc/rc.conf. For `hostA` this would look like:

```
network_interfaces="lo0 hatm0"
ifconfig_hatm0="inet 192.168.173.1 up"
natm_static_routes="hostB hostC hostD"
route_hostB="192.168.173.2 hatm0 0 100 llc/snap ubr"
route_hostC="192.168.173.3 hatm0 0 101 llc/snap ubr"
route_hostD="192.168.173.4 hatm0 0 102 llc/snap ubr"
```

The current state of all CLIP routes can be obtained with:

```
hostA# atmconfig natm show
```

56.12. Common Access Redundancy Protocol (CARP)

The Common Access Redundancy Protocol, or CARP allows multiple hosts to share the same IP address. In some configurations, this may be used for availability or load balancing. Hosts may use separate IP addresses as well, as in the example provided here.

To enable support for CARP, the FreeBSD kernel must be rebuilt with the following option:

```
device  carp
```

CARP functionality should now be available and may be tuned via several `sysctl` OIDs. Devices themselves may be loaded via the `ifconfig` command:

```
# ifconfig carp0 create
```

In a real environment, these interfaces will need unique identification numbers known as a VHID. This VHID or Virtual Host Identification will be used to distinguish the host on the network.

56.12.1. Using CARP For Server Availability (CARP)

One use of CARP, as noted above, is for server availability. This example will provide failover support for three hosts, all with unique IP addresses and providing the same web content. These machines will act in conjunction with a Round Robin DNS configuration. The failover machine will have two additional CARP interfaces, one for each of the content server's IPs. When a failure occurs, the failover server should pick up the failed machine's IP address. This means the failure should go completely unnoticed to the user. The failover server requires identical content and services as the other content servers it is expected to pick up load for.

The two machines should be configured identically other than their issued hostnames and VHIDs. This example calls these machines `hosta.example.org` and `hostb.example.org` respectively. First, the required lines for a CARP configuration have to be added to rc.conf. For `hosta.example.org`, the rc.conf file should contain the following lines:

```
hostname="hosta.example.org"
ifconfig_fxp0="inet 192.168.1.3 netmask 255.255.255.0"
cloned_interfaces="carp0"
ifconfig_carp0="vhid 1 pass testpast 192.168.1.50/24"
```

On `hostb.example.org` the following lines should be in rc.conf:

```
hostname="hostb.example.org"
ifconfig_fxp0="inet 192.168.1.4 netmask 255.255.255.0"
cloned_interfaces="carp0"
ifconfig_carp0="vhid 2 pass testpass 192.168.1.51/24"
```

It is very important that the passwords, specified by the `pass` option to `ifconfig`, are identical. The carp devices will only listen to and accept advertisements from machines with the correct password. The VHID must also be different for each machine.

The third machine, `provider.example.org`, should be prepared so that it may handle failover from either host. This machine will require two carp devices, one to handle each host. The appropriate

rc.conf configuration lines will be similar to the following:

```
hostname="provider.example.org"
ifconfig_fxp0="inet 192.168.1.5 netmask 255.255.255.0"
cloned_interfaces="carp0 carp1"
ifconfig_carp0="vhid 1 advskew 100 pass testpass 192.168.1.50/24"
ifconfig_carp1="vhid 2 advskew 100 pass testpass 192.168.1.51/24"
```

Having the two carp devices will allow `provider.example.org` to notice and pick up the IP address of either machine should it stop responding.

The default FreeBSD kernel *may* have preemption enabled. If so, `provider.example.org` may not relinquish the IP address back to the original content server. In this case, an administrator may "nudge" the interface. The following command should be issued on `provider.example.org`:

```
# ifconfig carp0 down && ifconfig carp0 up
```

This should be done on the carp interface which corresponds to the correct host.

At this point, CARP should be completely enabled and available for testing. For testing, either networking has to be restarted or the machines need to be rebooted.

More information is always available in the carp(4) manual page.

params: path: "/books/handbook/partv/" :sectnums!: :leveloffset: +1

Appendix A: Που θα Βρείτε το FreeBSD

Chapter 57. Εκδόσεις σε CDROM και DVD

57.1. Retail Εκδόσεις

Το FreeBSD είναι διαθέσιμο ως εμπορικό προϊόν (FreeBSD CD, επιπρόσθετο λογισμικό, και τυπωμένη τεκμηρίωση) από διάφορους προμηθευτές:

- Frys Electronics
  WWW: http://www.frys.com/

57.2. CD και DVD διανομές

Το FreeBSD είναι διαθέσιμο σε CD και DVD για αγορά μέσω διαδικτύου από τους παρακάτω προμηθευτές:

- FreeBSD Mall, Inc.
  1164 Claremont Dr
  Brentwood, CA
  94513
  USA
  Τηλέφωνο: +1 925 240-6652
  Fax: +1 925 674-0821
  Email: info@freebsdmall.com
  WWW: https://www.freebsdmall.com
- Getlinux
  WWW: https://www.getlinux.fr/
- Dr. Hinner EDV
  Schäftlarnstr. 10 // 4. Stock
  D-81371 München
  Germany
  Τηλέφωνο: +49 171 417 544 6
  Email: infow@hinner.de
  WWW: http://www.hinner.de/linux/freebsd.html
- JMC Software
  Ireland
  Τηλέφωνο: 353 1 6291282
  WWW: http://www.thelinuxmall.com
- Linux Distro UK
  42 Wharfedale Road
  Margate
  CT9 2TB
  United Kingdom
  WWW: https://linux-distro.co.uk/
- The Linux Emporium
  Hilliard House, Lester Way

Wallingford
OX10 9TA
United Kingdom
Τηλέφωνο: +44 1491 837010
Fax: +44 1491 837016
WWW: http://www.linuxemporium.co.uk/products/bsd/

- Linux+ DVD Magazine
  Lewartowskiego 6
  Warsaw
  00-190
  Poland
  Τηλέφωνο: +48 22 860 18 18
  Email: <editors@lpmagazine.org>
  WWW: http://www.lpmagazine.org/
- Linux System Labs Australia
  21 Ray Drive
  Balwyn North
  VIC - 3104
  Australia
  Τηλέφωνο: +61 3 9857 5918
  Fax: +61 3 9857 8974
  WWW: http://www.lsl.com.au
- LinuxCenter.Ru
  Galernaya Street, 55
  Saint-Petersburg
  190000
  Russia
  Τηλέφωνο: +7-812-3125208
  Email: <info@linuxcenter.ru>
  WWW: http://linuxcenter.ru/shop/freebsd

57.3. Διανομείς

Αν είστε μεταπωλητής και μπορείτε να διανείμετε σε CD-ROM προϊόντα βασισμένα στο FreeBSD, παρακαλούμε επικοινωνήστε με κάποιον από τους διανομείς:

- Ingram Micro
  1600 E. St. Andrew Place
  Santa Ana, CA 92705-4926
  USA
  Τηλέφωνο: 1 (800) 456-8000
  WWW: http://www.ingrammicro.com/
- Kudzu, LLC
  7375 Washington Ave. S.
  Edina, MN 55439
  USA

Τηλέφωνο: +1 952 947-0822
Fax: +1 952 947-0876
Email: <sales@kudzuenterprises.com>

- LinuxCenter.Ru
  Galernaya Street, 55
  Saint-Petersburg
  190000
  Russia
  Τηλέφωνο: +7-812-3125208
  Email: <info@linuxcenter.ru>
  WWW: http://linuxcenter.ru/freebsd

Chapter 58. Εξυπηρετητές FTP

Οι επίσημες εκδόσεις του FreeBSD είναι διαθέσιμες μέσω ανώνυμης FTP σύνδεσης από διάφορους εξυπηρετητές FTP σε όλο τον κόσμο. Ο κεντρικός εξυπηρετητής ftp://ftp.FreeBSD.org/pub/FreeBSD/ έχει πολύ καλή σύνδεση με τον υπόλοιπο κόσμο, και επιτρέπει ένα μεγάλο αριθμό ταυτόχρονων συνδέσεων. Ακόμα κι έτσι όμως, είναι μάλλον καλή ιδέα να βρείτε κάποιο εξυπηρετητή FTP που είναι πιο "κοντά" σας (ειδικά αν θέλετε να στήσετε κάποιο τοπικό mirror site).

Το FreeBSD είναι επίσης διαθέσιμο μέσω σύνδεσης ανώνυμου FTP από τα παρακάτω mirror sites. Αν επιλέξετε να κατεβάσετε το FreeBSD μέσω ανώνυμου FTP, σας παρακαλούμε να διαλέξετε κάποιο εξυπηρετητή ο οποίος είναι κοντά σας. Τα mirror sites που αναφέρονται ως "Κύρια Mirror Sites" έχουν συνήθως την πλήρη συλλογή αρχείων του FreeBSD (όλες τις διαθέσιμες εκδόσεις, για κάθε διαθέσιμη αρχιτεκτονική συστήματος), αλλά είναι πιθανόν να πετύχετε καλύτερες ταχύτητες εξυπηρέτησης με κάποιο εξυπηρετητή που είναι στη δική σας χώρα ή περιοχή. Τα τοπικά sites έχουν συνήθως τις πιο πρόσφατες εκδόσεις για τις πιο δημοφιλείς αρχιτεκτονικές συστήματος, οπότε μπορεί να μην έχουν όλες τις πιθανές εκδόσεις του FreeBSD. Όλα τα sites δέχονται συνδέσεις μέσω ανώνυμου FTP. Μερικά από αυτά μπορεί να υποστηρίζουν και άλλης μορφής συνδέσεις. Οι εναλλακτικές μορφές σύνδεσης αναφέρονται ξεχωριστά για κάθε site παρακάτω:

Central Servers, Primary Mirror Sites, Armenia, Australia, {mirrors-austria}, Brazil, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Ireland, Japan, Korea, Latvia, Lithuania, Netherlands, New Zealand, Norway, Poland, Russia, Saudi Arabia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, Ukraine, United Kingdom, United States of America.

(as of UTC)

Central Servers

ftp://ftp.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp.FreeBSD.org/pub/FreeBSD/ / http://ftp.FreeBSD.org/pub/FreeBSD/)

Primary Mirror Sites

In case of problems, please contact the hostmaster <mirror-admin@FreeBSD.org> for this domain.

- ftp://ftp1.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp4.FreeBSD.org/pub/FreeBSD/ / http://ftp4.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp10.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp10.FreeBSD.org/pub/FreeBSD/ / http://ftp10.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp11.FreeBSD.org/pub/FreeBSD/ (ftp)

- ftp://ftp13.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp14.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp14.FreeBSD.org/pub/FreeBSD/)

Armenia

In case of problems, please contact the hostmaster <hostmaster@am.FreeBSD.org> for this domain.

- ftp://ftp1.am.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp1.am.FreeBSD.org/pub/FreeBSD/ / rsync)

Australia

In case of problems, please contact the hostmaster <hostmaster@au.FreeBSD.org> for this domain.

- ftp://ftp.au.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.au.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.au.FreeBSD.org/pub/FreeBSD/ (ftp)

{mirrors-austria}

In case of problems, please contact the hostmaster <{mirrors-austria-email}> for this domain.

- {mirrors-austria-ftp} (ftp / ftpv6 / {mirrors-austria-ftp-http} / {mirrors-austria-ftp-httpv6})

Brazil

In case of problems, please contact the hostmaster <hostmaster@br.FreeBSD.org> for this domain.

- ftp://ftp2.br.FreeBSD.org/FreeBSD/ (ftp / http://ftp2.br.FreeBSD.org/)
- ftp://ftp3.br.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp4.br.FreeBSD.org/pub/FreeBSD/ (ftp)

Czech Republic

In case of problems, please contact the hostmaster <hostmaster@cz.FreeBSD.org> for this domain.

- ftp://ftp.cz.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp.cz.FreeBSD.org/pub/FreeBSD/ / http://ftp.cz.FreeBSD.org/pub/FreeBSD/ / http://ftp.cz.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp2.cz.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.cz.FreeBSD.org/pub/FreeBSD/)

Denmark

In case of problems, please contact the hostmaster <staff@dotsrc.org> for this domain.

- ftp://ftp.dk.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp.dk.FreeBSD.org/pub/FreeBSD/ / http://ftp.dk.FreeBSD.org/pub/FreeBSD/)

Estonia

In case of problems, please contact the hostmaster <hostmaster@ee.FreeBSD.org> for this domain.

- ftp://ftp.ee.FreeBSD.org/pub/FreeBSD/ (ftp)

Finland

In case of problems, please contact the hostmaster <hostmaster@fi.FreeBSD.org> for this domain.

- ftp://ftp.fi.FreeBSD.org/pub/FreeBSD/ (ftp)

France

In case of problems, please contact the hostmaster <hostmaster@fr.FreeBSD.org> for this domain.

- ftp://ftp.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp1.fr.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp1.fr.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp3.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.fr.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp7.fr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.fr.FreeBSD.org/pub/FreeBSD/ (ftp)

Germany

In case of problems, please contact the hostmaster <de-bsd-hubs@de.FreeBSD.org> for this domain.

- ftp://ftp.de.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp1.de.FreeBSD.org/freebsd/ (ftp / http://www1.de.FreeBSD.org/freebsd/ / rsync://rsync3.de.FreeBSD.org/freebsd/)
- ftp://ftp2.de.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.de.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp4.de.FreeBSD.org/FreeBSD/ (ftp / http://ftp4.de.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.de.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.de.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp7.de.FreeBSD.org/pub/FreeBSD/)

Greece

In case of problems, please contact the hostmaster <hostmaster@gr.FreeBSD.org> for this domain.

- ftp://ftp.gr.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.gr.FreeBSD.org/pub/FreeBSD/ (ftp)

Hong Kong

ftp://ftp.hk.FreeBSD.org/pub/FreeBSD/ (ftp)

Ireland

In case of problems, please contact the hostmaster <hostmaster@ie.FreeBSD.org> for this domain.

- ftp://ftp3.ie.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)

Japan

In case of problems, please contact the hostmaster <hostmaster@jp.FreeBSD.org> for this domain.

- ftp://ftp.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp7.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.jp.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp9.jp.FreeBSD.org/pub/FreeBSD/ (ftp)

Korea

In case of problems, please contact the hostmaster <hostmaster@kr.FreeBSD.org> for this domain.

- ftp://ftp.kr.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)
- ftp://ftp2.kr.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.kr.FreeBSD.org/pub/FreeBSD/)

Latvia

In case of problems, please contact the hostmaster <hostmaster@lv.FreeBSD.org> for this domain.

- ftp://ftp.lv.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.lv.FreeBSD.org/pub/FreeBSD/)

Lithuania

In case of problems, please contact the hostmaster <hostmaster@lt.FreeBSD.org> for this domain.

- ftp://ftp.lt.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.lt.FreeBSD.org/pub/FreeBSD/)

Netherlands

In case of problems, please contact the hostmaster <hostmaster@nl.FreeBSD.org> for this domain.

- ftp://ftp.nl.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.nl.FreeBSD.org/os/FreeBSD/ / rsync)
- ftp://ftp2.nl.FreeBSD.org/pub/FreeBSD/ (ftp)

New Zealand

- ftp://ftp.nz.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.nz.FreeBSD.org/pub/FreeBSD/)

Norway

In case of problems, please contact the hostmaster <hostmaster@no.FreeBSD.org> for this domain.

- ftp://ftp.no.FreeBSD.org/pub/FreeBSD/ (ftp / rsync)

Poland

In case of problems, please contact the hostmaster <hostmaster@pl.FreeBSD.org> for this domain.

- ftp://ftp.pl.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp2.pl.FreeBSD.org

Russia

In case of problems, please contact the hostmaster <hostmaster@ru.FreeBSD.org> for this domain.

- ftp://ftp.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ru.FreeBSD.org/FreeBSD/ / rsync)
- ftp://ftp2.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp2.ru.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp5.ru.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp5.ru.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp6.ru.FreeBSD.org/pub/FreeBSD/ (ftp)

Saudi Arabia

In case of problems, please contact the hostmaster <ftpadmin@isu.net.sa> for this domain.

- ftp://ftp.isu.net.sa/pub/ftp.freebsd.org (ftp)

Slovenia

In case of problems, please contact the hostmaster <hostmaster@si.FreeBSD.org> for this domain.

- ftp://ftp.si.FreeBSD.org/pub/FreeBSD/ (ftp)

South Africa

In case of problems, please contact the hostmaster <hostmaster@za.FreeBSD.org> for this domain.

- {mirrors-south-africa-ftp} (ftp)
- ftp://ftp2.za.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.za.FreeBSD.org/pub/FreeBSD/ (ftp)

Spain

In case of problems, please contact the hostmaster <hostmaster@es.FreeBSD.org> for this domain.

- ftp://ftp.es.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.es.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp3.es.FreeBSD.org/pub/FreeBSD/ (ftp)

Sweden

In case of problems, please contact the hostmaster <hostmaster@se.FreeBSD.org> for this domain.

- ftp://ftp.se.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.se.FreeBSD.org/pub/FreeBSD/ (ftp / rsync://ftp2.se.FreeBSD.org/)
- ftp://ftp3.se.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.se.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp4.se.FreeBSD.org/pub/FreeBSD/ / http://ftp4.se.FreeBSD.org/pub/FreeBSD/ / http://ftp4.se.FreeBSD.org/pub/FreeBSD/ / rsync://ftp4.se.FreeBSD.org/pub/FreeBSD/ / rsync://ftp4.se.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp6.se.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.se.FreeBSD.org/pub/FreeBSD/)

Switzerland

In case of problems, please contact the hostmaster <hostmaster@ch.FreeBSD.org> for this domain.

- ftp://ftp.ch.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ch.FreeBSD.org/pub/FreeBSD/)

Taiwan

In case of problems, please contact the hostmaster <hostmaster@tw.FreeBSD.org> for this domain.

- ftp://ftp.ch.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp.tw.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp2.tw.FreeBSD.org/pub/FreeBSD/ (ftp / ftp://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / http://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / http://ftp2.tw.FreeBSD.org/pub/FreeBSD/ / rsync / rsyncv6)
- ftp://ftp4.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.tw.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.tw.FreeBSD.org/ / rsync)
- ftp://ftp7.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp11.tw.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp11.tw.FreeBSD.org/FreeBSD/)
- ftp://ftp12.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp13.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp14.tw.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp15.tw.FreeBSD.org/pub/FreeBSD/ (ftp)

Ukraine

- ftp://ftp.ua.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp.ua.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp6.ua.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp6.ua.FreeBSD.org/pub/FreeBSD / rsync://ftp6.ua.FreeBSD.org/FreeBSD/)
- ftp://ftp7.ua.FreeBSD.org/pub/FreeBSD/ (ftp)

United Kingdom

In case of problems, please contact the hostmaster <hostmaster@uk.FreeBSD.org> for this domain.

- ftp://ftp.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.uk.FreeBSD.org/pub/FreeBSD/ (ftp / rsync://ftp2.uk.FreeBSD.org/ftp.freebsd.org/pub/FreeBSD/)
- ftp://ftp3.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.uk.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp5.uk.FreeBSD.org/pub/FreeBSD/ (ftp)

United States of America

In case of problems, please contact the hostmaster <hostmaster@us.FreeBSD.org> for this domain.

- ftp://ftp1.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp2.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp3.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp4.us.FreeBSD.org/pub/FreeBSD/ (ftp / ftpv6 / http://ftp4.us.FreeBSD.org/pub/FreeBSD/ / http://ftp4.us.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp5.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp6.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp8.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp10.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp11.us.FreeBSD.org/pub/FreeBSD/ (ftp)
- ftp://ftp13.us.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp13.us.FreeBSD.org/pub/FreeBSD/ / rsync)
- ftp://ftp14.us.FreeBSD.org/pub/FreeBSD/ (ftp / http://ftp14.us.FreeBSD.org/pub/FreeBSD/)
- ftp://ftp15.us.FreeBSD.org/pub/FreeBSD/ (ftp)

Chapter 59. Ανώνυμο CVS

59.1. Εισαγωγή

Η σύνδεση ανώνυμου CVS (ή *anoncvs* όπως λέγεται μερικές φορές) υποστηρίζεται από τα εργαλεία CVS που διανέμονται με το ίδιο το FreeBSD για συγχρονισμό τοπικών αρχείων με ένα απομακρυσμένο repository. Ένα από τα χαρακτηριστικά του CVS είναι ότι επιτρέπει στους χρήστες του FreeBSD να συγχρονίζουν, χωρίς ιδιαίτερα δικαιώματα χρήστη, τα τοπικά αντίγραφα πηγαίου κώδικα που έχουν με τους κεντρικούς, επίσημους εξυπηρετητές CVS του FreeBSD project. Για να χρησιμοποιήσει κανείς το CVS αρκεί: (α) να ορίσει την τιμή της μεταβλητής περιβάλλοντος `CVSROOT` έτσι ώστε να δείχνει προς έναν από τους επίσημους εξυπηρετητές, και (β) να δώσει τον κωδικό "anoncvs" στην προτροπή της εντολής `cvs login`. Τότε μπορεί να χρησιμοποιήσει το εργαλείο cvs(1) για να προσπελάσει το απομακρυσμένο CVS repository του FreeBSD σαν ένα οποιοδήποτε τοπικό repository.

Η εντολή `cvs login` αποθηκεύει τους κωδικούς που χρησιμοποιούνται για πιστοποίησης της ταυτότητάς σας στον εξυπηρετητή CVS σε ένα αρχείο με όνομα .cvspass στον `HOME` κατάλογο του τοπικού σας λογαριασμού. Αν αυτό το αρχείο δεν υπάρχει ήδη, μπορεί να αποτύχει η εντολή `cvs login` την πρώτη φορά. Μπορείτε απλά να δημιουργήσετε ένα άδειο αρχείο .cvspass και να ξανατρέξετε την εντολή `cvs login`.

Μπορεί να πει κανείς ότι το CVSup και το *anoncvs* είναι ουσιαστικά παρόμοιοι τρόποι συγχρονισμού αρχείων και υποστηρίζουν την ίδια λειτουργικότητα, αλλά υπάρχουν κάποιες διαφορές οι οποίες μπορεί να παίξουν σημαντικό ρόλο στην επιλογή μεταξύ αυτών των δύο μεθόδων. Γενικά, το CVSup κάνει πολύ πιο αποδοτική χρήση της σύνδεσης που έχετε και χρησιμοποιεί ένα πολύ πιο έξυπνο πρωτόκολλο επικοινωνίας, αλλά υπάρχει και το αντίστοιχο τίμημα. Για να χρησιμοποιήσετε το CVSup πρέπει να εγκαταστήσετε και να ρυθμίσετε ένα ειδικό πρόγραμμα πελάτη, και τότε μπορείτε να συγχρονίσετε μόνο μεγάλες συλλογές αρχείων - τις οποίες το CVSup αποκαλεί "συλλογές" (collections).

Το anoncvs, από την άλλη, μπορεί να χρησιμοποιηθεί για να εξετάσει κανείς τις αλλαγές ενός και μόνο αρχείου ή ενός μόνο προγράμματος και των συνοδευτικών του αρχείων (π.χ. τον πηγαίο κώδικα της εντολής `ls` ή της `grep`), με χρήση του ονόματος του κατάλληλου module. Το anoncvs είναι πιο βολικό για εργασίες που απαιτούν βέβαια μόνο ανάγνωση. Οπότε, αν θέλετε να υποστηρίξετε την ανάπτυξη προγραμμάτων τοπικά, το CVSup είναι μάλλον μονόδρομος.

59.2. Χρησιμοποιώντας Ανώνυμο CVS

Η ρύθμιση του cvs(1) ώστε να χρησιμοποιεί ένα ανώνυμο CVS repository γίνεται απλώς ρυθμίζοντας την μεταβλητή περιβάλλοντος `CVSROOT` ώστε να δείχνει σε έναν από τους *anoncvs* εξυπηρετητές του FreeBSD project. Την ώρα που γράφονται αυτές οι γραμμές, είναι διαθέσιμοι οι ακόλουθοι εξυπηρετητές:

- *Γαλλία*: :pserver:anoncvs@anoncvs.fr.FreeBSD.org:/home/ncvs (Για pserver χρησιμοποιήστε την εντολή `cvs login` και δώστε τον κωδικό "anoncvs" όταν σας ζητηθεί. Το ssh δεν απαιτεί τη χρήση κωδικού.)

- *Ταΐβάν*: :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs (Για pserver χρησιμοποιήστε την εντολή `cvs login` και δώστε οτιδήποτε για κωδικό όταν σας ζητηθεί, Το ssh δεν απαιτεί τη χρήση κωδικού.)

```
SSH2 HostKey: 1024 02:ed:1b:17:d6:97:2b:58:5e:5c:e2:da:3b:89:88:26
/etc/ssh/ssh_host_rsa_key.pub
SSH2 HostKey: 1024 e8:3b:29:7b:ca:9f:ac:e9:45:cb:c8:17:ae:9b:eb:55
/etc/ssh/ssh_host_dsa_key.pub
```

Καθώς το CVS σας επιτρέπει να κάνετε "check out" ουσιαστικά οποιαδήποτε έκδοση του πηγαίου κώδικα του FreeBSD υπήρξε ποτέ (και σε ορισμένες περιπτώσεις ακόμα και εκδόσεις που δεν έχουν κυκλοφορήσει ακόμα), θα πρέπει να είστε εξοικειωμένος με την επιλογή του cvs(1) με την οποία επιλέγεται το revision (πρόκειται για την `-r`) και ποιες είναι οι επιτρεπτές τιμές της για το repository του FreeBSD project.

Υπάρχουν δύο είδη tags (ετικετών), τα revision tags (ετικέτες έκδοσης) και τα branch tags. Ένα revision tag αναφέρεται σε μια συγκεκριμένη έκδοση. Η έννοια του παραμένει σταθερή μέρα με τη μέρα. Από την άλλη, ένα branch tag δείχνει την τελευταία έκδοση μιας συγκεκριμένης πορείας ανάπτυξης, σε κάθε χρονική στιγμή. Καθώς το branch tag δεν αναφέρεται σε κάποια συγκεκριμένη έκδοση, μπορεί αύριο να σημαίνει κάτι διαφορετικό από ότι σημαίνει σήμερα.

Το Ετικέτες (Tags) για το CVS περιέχει revision tags τα οποία μπορεί να ενδιαφέρουν τους χρήστες. Υπενθυμίζουμε ότι κανένα από αυτά δεν είναι έγκυρο για την Συλλογή των Ports, καθώς αυτή δεν έχει πολλαπλές εκδόσεις (revisions).

Όταν καθορίζετε κάποιο branch tag, φυσιολογικά λαμβάνετε τις τελευταίες εκδόσεις των αρχείων που υπάρχουν σε αυτή τη γραμμή ανάπτυξης. Αν θέλετε να λάβετε κάποια παλιότερη έκδοση, μπορείτε χρησιμοποιώντας την ημερομηνία σε συνδυασμό με την επιλογή `-D date`. Δείτε τη σελίδα manual του cvs(1) για περισσότερες λεπτομέρειες.

59.3. Παραδείγματα

Αν και πραγματικά συνίσταται να διαβάσετε προσεκτικά τη σελίδα manual του cvs(1) πριν κάνετε οτιδήποτε, παρακάτω σας δίνουμε κάποια γρήγορα παραδείγματα τα οποία ουσιαστικά θα σας δείξουν πως να χρησιμοποιήσετε το Ανώνυμο CVS:

Παράδειγμα 28. Λήψη (Check out) Κάποιου Αρχείου από το -CURRENT (ls(1)):

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
Στην προτροπή, δώστε οποιαδήποτε λέξη για «password».
% cvs co ls
```

Παράδειγμα 29. Χρήση SSH για Λήψη (check out) του Δέντρου src/:

```
% cvs -d anoncvs@anoncvs1.FreeBSD.org:/home/ncvs co src
The authenticity of host 'anoncvs1.freebsd.org (216.87.78.137)' can't be
established.
DSA key fingerprint is 53:1f:15:a3:72:5c:43:f6:44:0e:6a:e9:bb:f8:01:62.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'anoncvs1.freebsd.org' (DSA) to the list of known
hosts.
```

Παράδειγμα 30. Λήψη της Έκδοσης του Αρχείου ls(1) από το 8-STABLE Branch:

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
Στην προτροπή, δώστε οποιαδήποτε λέξη για «password».
% cvs co -rRELENG_8 ls
```

Παράδειγμα 31. Δημιουργία μιας Λίστας Αλλαγών (ως Unified Diffs) της ls(1):

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
Στην προτροπή, δώστε οποιαδήποτε λέξη για «password».
% cvs rdiff -u -rRELENG_8_0_0_RELEASE -rRELENG_8_1_0_RELEASE ls
```

Παράδειγμα 32. Βρίσκοντας Ποια Άλλα Ονόματα Modules μπορούν να Χρησιμοποιηθούν:

```
% setenv CVSROOT :pserver:anoncvs@anoncvs.tw.FreeBSD.org:/home/ncvs
% cvs login
Στην προτροπή, δώστε οποιαδήποτε λέξη για «password».
% cvs co modules
% more modules/modules
```

59.4. Άλλες Πηγές Πληροφοριών

Οι παρακάτω πηγές πληροφοριών ίσως σας φανούν χρήσιμες για να μάθετε το CVS:

- CVS Tutorial από το California Polytechnic State University.
- CVS Home, η ομάδα ανάπτυξης και υποστήριξης του CVS.
- CVSweb Διεπαφή Web για το CVS του FreeBSD Project.

Chapter 60. Χρησιμοποιώντας το CTM

Το CTM είναι μια μέθοδος να διατηρούμε σε συγχρονισμό ένα απομακρυσμένο κατάλογο με ένα κεντρικό. Αναπτύχθηκε για χρήση με το δέντρο πηγαίου κώδικα του FreeBSD, αν και άλλοι άνθρωποι μπορεί να το βρουν χρήσιμο και για διαφορετικούς σκοπούς καθώς περνάει ο καιρός. Τη δεδομένη στιγμή υπάρχει ελάχιστη ως ανύπαρκτη τεκμηρίωση για την διαδικασία δημιουργίας αρχείων διαφορών (deltas), και αν χρειάζεστε περισσότερες πληροφορίες, επικοινωνήστε με τη λίστα ταχυδρομείου ctm-users-desc ειδικά αν θέλετε να χρησιμοποιήσετε το CTM για άλλες εφαρμογές.

60.1. Γιατί Πρέπει να Χρησιμοποιήσω το CTM;

Το CTM θα σας δώσει ένα τοπικό αντίγραφο του δέντρου πηγαίου κώδικα του FreeBSD. Υπάρχει διαθέσιμος ένας αριθμός από "γεύσεις" του δέντρου. Το CTM μπορεί να σας παρέχει τις πληροφορίες που χρειάζεστε, είτε αποφασίσετε να παρακολουθείτε ολόκληρο το δέντρο, είτε κάποιο από τα παρακλάδια του. Αν ανήκετε στα ενεργά μέλη ανάπτυξης του FreeBSD αλλά έχετε κακής ποιότητας (ή καθόλου) TCP/IP συνδεσιμότητα, ή απλά θέλετε οι αλλαγές να σας έρχονται αυτόματα, το CTM έχει φτιαχτεί για σας. Θα χρειαστεί να παίρνετε ως τρία deltas την ημέρα για τα κλαδιά του δέντρου που έχουν την πιο ενεργή ανάπτυξη. Θα πρέπει ωστόσο να θεωρήσετε ως καλύτερη λύση την αυτόματη αποστολή τους μέσω email. Τα μεγέθη των ανανεώσεων κρατούνται πάντα όσο το δυνατόν πιο μικρά. Συνήθως είναι μικρότερα από 5K, περιστασιακά (ένα στα δέκα) είναι από 10-50K και ορισμένες φορές εμφανίζονται και κάποια που είναι 100K ή και μεγαλύτερα.

Θα πρέπει επίσης να εξοικειωθείτε με τις διάφορες παγίδες που σχετίζονται με την απευθείας εργασία στον υπό ανάπτυξη πηγαίο κώδικα σε σχέση με μια έτοιμη, προκατασκευασμένη έκδοση. Αυτό ισχύει ακόμα περισσότερο αν επιλέξετε να χρησιμοποιήσετε τον πηγαίο κώδικα από το "current". Σας συνιστούμε να διαβάσετε πως να χρησιμοποιήσετε το current στο FreeBSD.

60.2. Τι Χρειάζομαι για να Χρησιμοποιήσω το CTM;

Θα χρειαστείτε δύο πράγματα: Την εφαρμογή CTM και τις αρχικές αλλαγές (deltas) για να τις εισάγετε σε αυτήν (ώστε να φτάσετε στο επίπεδο του "current").

Το CTM είναι μέρος του FreeBSD από την έκδοση 2.0, και βρίσκεται στον κατάλογο /usr/src/usr.sbin/ctm εφόσον έχετε εγκατεστημένο τον πηγαίο κώδικα.

Τα "deltas" με τα οποία τροφοδοτείτε το CTM μπορείτε να τα αποκτήσετε με δύο τρόπους, μέσω FTP ή μέσω email. Αν έχετε γενική FTP πρόσβαση στο Internet, θα βρείτε υποστήριξη για το CTM στις ακόλουθες τοποθεσίες FTP:

ftp://ftp.FreeBSD.org/pub/FreeBSD/CTM/

ή δείτε το τμήμα mirrors.

Κάντε FTP στο σχετικό κατάλογο και διαβάστε το αρχείο README για να ξεκινήσετε.

Αν θέλετε να λαμβάνετε τα deltas μέσω email:

Γραφτείτε συνδρομητής σε μια από τις λίστες διανομής του CTM. Η λίστα ctm-cvs-cur-desc υποστηρίζει ολόκληρο το δέντρο του CVS. Η λίστα ctm-src-cur-desc υποστηρίζει την κεφαλή (head) του κλάδου ανάπτυξης (development branch). Η λίστα ctm-src-7-desc υποστηρίζει την έκδοση 7.X κ.ο.κ. Αν δεν γνωρίζετε πως να εγγραφείτε σε μια λίστα, κάντε κλικ στο όνομα της λίστας που εμφανίζεται παραπάνω ή πηγαίνετε στο https://lists.freebsd.org και κάντε κλικ στη λίστα που θέλετε να εγγραφείτε. Η σελίδα της λίστας θα πρέπει να περιέχει όλες τις απαραίτητες πληροφορίες σχετικά με τις συνδρομές.

Όταν αρχίσετε να λαμβάνετε ανανεώσεις CTM μέσω mail, μπορείτε να χρησιμοποιήσετε το πρόγραμμα `ctm_rmail` για να τις αποσυμπιέσετε και να τις εφαρμόσετε. Μπορείτε στην πραγματικότητα να χρησιμοποιήσετε το πρόγραμμα `ctm_rmail` απευθείας μέσω μιας εγγραφής στο /etc/aliases αν θέλετε η διαδικασία να εκτελείται αυτοματοποιημένα. Δείτε τη σελίδα manual του `ctm_rmail` για περισσότερες λεπτομέρειες.

Άσχετα με τη μέθοδο που θα χρησιμοποιήσετε για να λάβετε τα deltas του CTM θα πρέπει να εγγραφείτε στη λίστα ctm-announce-desc. Στο μέλλον, αυτό θα είναι και το μόνο μέρος στο οποίο θα δημοσιεύονται πληροφορίες σχετικά με τις λειτουργίες του συστήματος CTM. Κάντε κλικ στο όνομα της παραπάνω λίστας, και ακολουθείστε τις οδηγίες για να εγγραφείτε.

60.3. Χρησιμοποιώντας το CTM για Πρώτη Φορά

Πριν αρχίσετε να χρησιμοποιείτε CTM deltas, θα πρέπει να έχετε ένα σημείο εκκίνησης για τα delta που έχουν δημιουργηθεί μετά από αυτό.

Θα πρέπει πρώτα να καθορίσετε τι έχετε ήδη. Οποιοσδήποτε μπορεί να αρχίσει από ένα "άδειο" κατάλογο. Θα πρέπει να ξεκινήσετε με ένα αρχικό "Κενό" delta για να αρχίσετε με το CTM δέντρο σας. Από κάποιο σημείο θεωρούμε ότι ένα από αυτά τα "αρχικά" deltas θα διανέμονται σε CD για τη δική σας διευκόλυνση, ωστόσο αυτό δεν συμβαίνει τη δεδομένη στιγμή.

Καθώς τα δέντρα είναι αρκετές δεκάδες megabytes, είναι προτιμότερο να ξεκινήσετε από κάτι που έχετε ήδη. Αν έχετε CD κάποιας διανομής (RELEASE), μπορείτε να αντιγράψετε ή να αποσυμπιέσετε από εκεί τον αρχικό πηγαίο κώδικα. Έτσι θα γλυτώσετε σημαντικό μέρος της μεταφοράς δεδομένων.

Μπορείτε να αναγνωρίσετε αυτά τα "αρχικά" deltas από το `X` που ακολουθεί τον αριθμό τους (για παράδειγμα src-cur.3210XEmpty.gz). Ο χαρακτηρισμός μετά το `X` αντιστοιχεί στην πηγή του αρχικού σας "seed". Το Empty είναι ένας άδειος κατάλογος. Κατά κανόνα δημιουργείται μια μετάβαση από το `Empty` κάθε 100 deltas. Επίσης τα αρχεία αυτά είναι μεγάλα! Συνηθισμένο μέγεθος για XEmpty deltas είναι τα 70 ως 80 MB συμπιεσμένων με `gzip` δεδομένων.

Μόλις επιλέξετε ένα βασικό delta για να ξεκινήσετε, θα χρειαστείτε επίσης όλα τα deltas με μεγαλύτερους από αυτό αριθμούς.

60.4. Χρησιμοποιώντας το CTM στην Καθημερινή σας Ζωή

Για να εφαρμόσετε τα deltas, απλώς γράψτε:

```
# cd /where/ever/you/want/the/stuff
# ctm -v -v /where/you/store/your/deltas/src-xxx.*
```

Το CTM αντιλαμβάνεται deltas τα οποία έχουν συμπιεστεί μέσω `gzip`, και έτσι δεν χρειάζεται να χρησιμοποιήσετε την `gunzip`, γλυτώνοντας με αυτό τον τρόπο χώρο στο δίσκο.

Το CTM δεν πρόκειται να πειράξει τα αρχεία σας αν δεν είναι απόλυτα σίγουρο για τη διαδικασία ανανέωσης. Για να επαληθεύσετε ένα delta μπορείτε επίσης να χρησιμοποιήσετε την επιλογή `-c` και το CTM δεν θα πειράξει τίποτα, απλώς θα επαληθεύσει την ακεραιότητα του delta και θα δει αν μπορεί να το εφαρμόσει χωρίς προβλήματα στο τρέχον δέντρο.

Υπάρχουν και άλλες επιλογές στο CTM, δείτε τις αντίστοιχες σελίδες manual ή κοιτάξτε τον πηγαίο κώδικα για περισσότερες πληροφορίες.

Αυτό είναι όλο στην πραγματικότητα. Κάθε φορά που λαμβάνετε ένα νέο delta, απλώς περάστε το στο CTM ώστε να έχετε πάντοτε ανανεωμένο τον πηγαίο σας κώδικα.

Μην σβήνετε τα deltas αν είναι δύσκολο να τα κατεβάσετε ξανά. Ίσως θέλετε να τα φυλάξετε για την περίπτωση που κάτι πάει στραβά. Ακόμα και αν το μόνο μέσο που έχετε είναι δισκέτες, κάντε αντίγραφο χρησιμοποιώντας την `fdwrite`.

60.5. Κρατώντας τις Τοπικές σας Αλλαγές

Ως προγραμματιστής, θα θέλετε να πειραματιστείτε και να αλλάξετε αρχεία στο δέντρο του πηγαίου κώδικα. Το CTM υποστηρίζει περιορισμένου τύπου τοπικές αλλαγές: πριν ελέγξει για την παρουσία ενός αρχείου foo, ελέγχει πρώτα για το foo.ctm. Αν το αρχείο αυτό υπάρχει, το CTM θα χρησιμοποιήσει αυτό αντί για το foo.

Η συμπεριφορά αυτή μας παρέχει ένα απλό τρόπο να διατηρήσουμε τοπικές αλλαγές: απλώς αντιγράψτε τα αρχεία που σκοπεύετε να αλλάξετε σε αντίστοιχα αρχεία με κατάληξη .ctm. Μπορείτε κατόπιν να κάνετε ότι αλλαγές θέλετε στον κώδικα ενώ το CTM θα διατηρεί ανανεωμένο το αρχείο .ctm.

60.6. Άλλες Ενδιαφέρουσες Επιλογές του CTM

60.6.1. Βρίσκοντας τι Ακριβώς θα Αλλάξει σε μια Ανανέωση

Μπορείτε να προσδιορίσετε τις αλλαγές που θα προκαλέσει το CTM στο repository του πηγαίου σας κώδικα, χρησιμοποιώντας την επιλογή `-l`.

Αυτό θα είναι χρήσιμο αν θέλετε να κρατήσετε ημερολόγιο των αλλαγών, αν θέλετε να επεξεργαστείτε τα τροποποιημένα αρχεία πριν ή μετά την τροποποίηση τους, ή αν απλώς αισθάνεστε ελαφρώς παρανοϊκός.

60.6.2. Δημιουργώντας Αντίγραφα Ασφαλείας πριν την Ανανέωση

Μερικές φορές θα θέλετε να κρατήσετε αντίγραφο ασφαλείας όλων των αρχείων που πρόκειται να

αλλαχθούν από μια ανανέωση μέσω CTM.

Δίνοντας την επιλογή `-B backup-file` το CTM θα δημιουργήσει αντίγραφο ασφαλείας όλων των αρχείων που πρόκειται να αλλαχθούν από κάποιο συγκεκριμένο delta στο αρχείο backup-file.

60.6.3. Περιορίζοντας τα Αρχεία που θα Αλλαχθούν από Κάποια Ανανέωση

Μερικές φορές ίσως να ενδιαφέρεστε να περιορίσετε την περιοχή δράσης μιας συγκεκριμένης ανανέωσης μέσω CTM ή ίσως σας ενδιαφέρει να πάρετε μόνο λίγα αρχεία από κάποια σειρά από deltas.

Μπορείτε να ελέγξετε τη λίστα των αρχείων στα οποία θα λειτουργήσει το CTM χρησιμοποιώντας ως φίλτρα, regular expressions με τις επιλογές `-e` και `-x`.

Για παράδειγμα, για να εξάγετε ένα ανανεωμένο αντίγραφο του αρχείου lib/libc/Makefile από την συλλογή σας των αποθηκευμένων CTM deltas, εκτελέστε τις εντολές:

```
# cd /where/ever/you/want/to/extract/it/
# ctm -e '^lib/libc/Makefile' ~ctm/src-xxx.*
```

Για κάθε αρχείο που καθορίζεται σε ένα CTM delta, οι επιλογές `-e` και `-x` εφαρμόζονται με τη σειρά που εμφανίζονται στη γραμμή εντολών. Στο αρχείο γίνεται επεξεργασία από το CTM, μόνο αν μαρκαριστεί ως έγκυρο προς ανανέωση μετά την εφαρμογή όλων των επιλογών `-e` και `-x`.

60.7. Μελλοντικά Σχέδια για το CTM

Είναι πάρα πολλά:

- Χρήση κάποιου είδους πιστοποίησης στο σύστημα CTM ώστε να αναγνωρίζονται τυχόν ψεύτικες ανανεώσεις.
- Ξεκαθάρισμα των επιλογών του CTM, καθώς προκαλούν σύγχυση και δεν είναι προφανείς.

60.8. Διάφορα

Υπάρχει επίσης και μια σειρά από deltas για την συλλογή των `ports`, αλλά δεν έχει εκδηλωθεί ακόμα αρκετό ενδιαφέρον για αυτή.

60.9. CTM Mirrors

Το CTM/FreeBSD διατίθεται μέσω ανώνυμου FTP από τα ακόλουθα mirrors. Αν επιλέξετε να κατεβάσετε το CTM μέσω ανώνυμου FTP, σας παρακαλούμε προσπαθήστε να επιλέξετε μια τοποθεσία κοντά σε σας.

Σε περίπτωση προβλημάτων, παρακαλούμε επικοινωνήστε με τη λίστα ctm-users-desc.

Καλιφόρνια, Bay Area, επίσημη πηγή

- ftp://ftp.FreeBSD.org/pub/FreeBSD/development/CTM/

Νότια Αφρική, αντίγραφα ασφαλείας για παλιά deltas

- ftp://ftp.za.FreeBSD.org/pub/FreeBSD/CTM/

Ταϊβάν/R.O.C.

- ftp://ctm.tw.FreeBSD.org/pub/FreeBSD/development/CTM/
- ftp://ctm2.tw.FreeBSD.org/pub/FreeBSD/development/CTM/
- ftp://ctm3.tw.FreeBSD.org/pub/FreeBSD/development/CTM/

Αν δεν βρήκατε κάποιο mirror στην περιοχή σας, ή αν το mirror δεν είναι πλήρες, προσπαθήστε να χρησιμοποιήσετε μια μηχανή αναζήτησης όπως η alltheweb.

Chapter 61. Χρησιμοποιώντας το CVSup

61.1. Εισαγωγή

Το CVSup είναι ένα λογισμικό για την διανομή και ανανέωση δέντρων πηγαίου κώδικα από ένα κεντρικό (master) CVS repository το οποίο βρίσκεται σε κάποιο απομακρυσμένο υπολογιστή. Το repository του FreeBSD βρίσκεται σε ένα κεντρικό μηχάνημα στην Καλιφόρνια. Με το CVSup, οι χρήστες του FreeBSD μπορούν εύκολα να διατηρήσουν ανανεωμένα τα αντίγραφα του πηγαίου τους κώδικα.

Το CVSup χρησιμοποιεί ένα μοντέλο ανανέωσης γνωστό ως *pull*. Στο μοντέλο αυτό, κάθε πελάτης ζητά τις ανανεώσεις από τον εξυπηρετητή, όταν και αν τις επιθυμεί. Ο εξυπηρετητής περιμένει, παθητικά, τις απαιτήσεις από τους πελάτες. Με τον τρόπο αυτό, κάθε ανανέωση ξεκινάει κατόπιν απαίτησης του πελάτη. Ο εξυπηρετητής ποτέ δεν στέλνει ανανεώσεις που δεν έχουν ζητηθεί. Οι χρήστες θα πρέπει είτε να εκτελέσουν το CVSup χειροκίνητα για να λάβουν μια ανανέωση, είτε θα πρέπει να ρυθμίσουν κατάλληλα το `cron` ώστε να το εκτελεί αυτόματα κατά τακτά χρονικά διαστήματα.

Ο όρος CVSup, γραμμένος με κεφαλαία και μικρά όπως φαίνεται, αναφέρεται σε ολόκληρο το πακέτο λογισμικού. Τα βασικά του τμήματα είναι η εντολή πελάτη `cvsup` η οποία εκτελείται στο μηχάνημα του κάθε χρήστη, και το πρόγραμμα του εξυπηρετητή `cvsupd` το οποίο εκτελείται σε κάθε ένα από τα mirror sites του FreeBSD.

Καθώς διαβάζετε την τεκμηρίωση και τις λίστες ταχυδρομείου του FreeBSD, μπορεί να βρείτε αναφορές στην εφαρμογή sup. Το sup ήταν ο πρόγονος του CVSup, και εξυπηρετούσε παρόμοιο σκοπό. Το CVSup χρησιμοποιείται με αρκετά όμοιο τρόπο με το sup, και στην πραγματικότητα, χρησιμοποιεί αρχεία ρυθμίσεων τα οποία έχουν πίσω συμβατότητα με αυτά του `sup`. Το sup δεν χρησιμοποιείται πλέον στο FreeBSD Project, επειδή το CVSup είναι ταχύτερο και προσφέρει μεγαλύτερη ευελιξία.

Το πρόγραμμα csup είναι το CVSup ξαναγραμμένο σε γλώσσα C. Το μεγαλύτερο του πλεονέκτημα είναι ότι είναι ταχύτερο, και δεν εξαρτάται από την γλώσσα προγραμματισμού Modula-3, την οποία και δεν χρειάζεται πλέον να εγκαταστήσετε. Επίσης μπορείτε να το χρησιμοποιήσετε άμεσα, καθώς περιλαμβάνεται στο βασικό σύστημα. Αν αποφασίσετε να χρησιμοποιήσετε το csup, απλώς παραλείψτε τα βήματα για την εγκατάσταση του CVSup και αντικαταστήστε κάθε αναφορά στο CVSup σε αυτό το άρθρο, με csup.

61.2. Εγκατάσταση

Ο ευκολότερος τρόπος για να εγκαταστήσετε το CVSup είναι μέσω του έτοιμου πακέτου net/cvsup από την συλλογή πακέτων του FreeBSD. Αν προτιμάτε να μεταγλωττίσετε το CVSup από τον πηγαίο κώδικα, μπορείτε να χρησιμοποιήσετε το port net/cvsup. Σας προειδοποιούμε ωστόσο ότι το port net/cvsup εξαρτάται από την Modula-3, η οποία χρειάζεται αρκετό χρόνο και χώρο στο δίσκο για να κατέβει και να μεταγλωττιστεί.

Αν πρόκειται να χρησιμοποιήσετε το CVSup σε ένα μηχάνημα το οποίο δεν θα

> διαθέτει γραφικό περιβάλλον μέσω του Xorg, όπως π.χ. σε ένα εξυπηρετητή, βεβαιωθείτε ότι εγκαθιστάτε το αντίστοιχο port το οποίο δεν περιλαμβάνει γραφικό περιβάλλον, δηλαδή το net/cvsup-without-gui.

61.3. Ρύθμιση του CVSup

Η λειτουργία του CVSup ελέγχεται από ένα αρχείο ρυθμίσεων που καλείται supfile. Υπάρχουν κάποια υποδείγματα από supfiles στον κατάλογο /usr/shared/examples/cvsup/.

Οι πληροφορίες στο supfile απαντούν τις ακόλουθες ερωτήσεις για το CVSup:

- Ποια αρχεία θέλετε να λάβετε;
- Ποιες εκδόσεις των αρχείων θέλετε;
- Από που θέλετε να τα λάβετε;
- Που θέλετε να τα αποθηκεύσετε στο μηχάνημα σας;
- Που θέλετε να αποθηκεύσετε τα αρχεία κατάστασης;

Στα επόμενα τμήματα, θα δημιουργήσουμε ένα τυπικό supfile απαντώντας κάθε μια από τις ερωτήσεις αυτές με τη σειρά. Πρώτα, θα περιγράψουμε τη συνολική δομή ενός supfile.

Ένα supfile είναι ένα αρχείο κειμένου. Τα σχόλια ξεκινάνε με `#` και επεκτείνονται ως το τέλος της γραμμής. Οι κενές γραμμές, καθώς και αυτές που περιέχουν μόνο σχόλια, αγνοούνται.

Κάθε γραμμή από τις υπόλοιπες περιγράφει ένα σετ αρχείων τα οποία επιθυμεί να λάβει ο χρήστης. Η γραμμή ξεκινάει με το όνομα μιας "συλλογής", ενός λογικού γκρουπ από αρχεία που ορίζεται από τον εξυπηρετητή. Το όνομα της συλλογής δηλώνει στον εξυπηρετητή ποια αρχεία επιθυμείτε. Μετά το όνομα της συλλογής, μπορεί να υπάρχουν από μηδέν ως κάποια πεδία, τα οποία χωρίζονται μεταξύ τους με κενά διαστήματα. Τα πεδία αυτά απαντούν τις ερωτήσεις που τέθηκαν παραπάνω. Υπάρχουν δύο τύποι πεδίων: πεδία σήμανσης (flags) και πεδία τιμών. Ένα πεδίο σήμανσης αποτελείται από μια μόνο λέξη κλειδί π.χ. `delete` ή `compress`. Ένα πεδίο τιμής ξεκινάει επίσης με μια λέξη κλειδί, αλλά αυτή ακολουθείτε χωρίς την παρεμβολή κενού διαστήματος από `=` και μια δεύτερη λέξη. Για παράδειγμα το `release=cvs` αποτελεί ένα πεδίο τιμής.

Ένα supfile τυπικά καθορίζει προς λήψη περισσότερες από μία συλλογές. Ένα τρόπος για να δομήσετε ένα supfile είναι να καθορίσετε όλα τα σχετικά πεδία χωριστά για κάθε συλλογή. Με τον τρόπο αυτό ωστόσο το supfile θα καταλάβει αρκετές γραμμές και θα είναι άβολο, επειδή τα περισσότερα πεδία είναι ίδια για όλες τις συλλογές που περιέχονται σε αυτό. Το CVSup παρέχει ένα μηχανισμό χρήσης προεπιλεγμένων τιμών, ώστε να αποφεύγονται αυτά τα προβλήματα. Οι γραμμές που ξεκινάνε με το ειδικό όνομα ψευτό-συλλογής `*default` μπορούν να χρησιμοποιηθούν για να θέσουν πεδία σήμανσης και τιμών τα οποία θα χρησιμοποιηθούν ως προεπιλογές για τις συλλογές του supfile που βρίσκονται μετά από αυτά. Μια προεπιλεγμένη τιμή μπορεί να αλλάξει αν καθοριστεί ξανά με νέα τιμή μέσα στην ίδια τη συλλογή. Οι προεπιλογές μπορούν επίσης να αλλάξουν, ή να προστεθούν νέες, βάζοντας πρόσθετα `*default` σε οποιοδήποτε σημείο μέσα στο supfile.

Γνωρίζοντας τα παραπάνω, θα προχωρήσουμε τώρα στη δόμηση ενός supfile για λήψη και ανανέωση του κυρίως δέντρου πηγαίου κώδικα για το FreeBSD-CURRENT.

- Ποια αρχεία θέλετε να λάβετε;

  Τα αρχεία που είναι διαθέσιμα μέσω της CVSup είναι οργανωμένα σε γκρουπ που ονομάζονται "συλλογές". Περιγραφή των διαθέσιμων συλλογών θα βρείτε στο ακόλουθο τμήμα. Στο παράδειγμα μας, θέλουμε να λάβουμε το πλήρες δέντρο πηγαίου κώδικα του FreeBSD συστήματος. Υπάρχει μια μεγάλη συλλογή `src-all` η οποία θα μας την δώσει όλη. Σαν πρώτο βήμα για την δόμηση του supfile, απλώς γράφουμε τις συλλογές, μία σε κάθε γραμμή (στην περίπτωση μας έχουμε μόνο μια γραμμή):

  ```
  src-all
  ```

- Ποιες εκδόσεις των αρχείων θέλετε να λάβετε;

  Με το CVSup, μπορείτε ουσιαστικά να λάβετε οποιαδήποτε έκδοση του πηγαίου κώδικα υπήρξε ποτέ. Αυτό είναι δυνατόν επειδή ο εξυπηρετητής cvsupd λειτουργεί απευθείας από το CVS repository, το οποίο περιέχει όλες τις εκδόσεις. Δηλώνετε ποια από αυτές θέλετε χρησιμοποιώντας τα πεδία τιμών `tag=` και `date=`.

  Θα πρέπει να δώσετε ιδιαίτερη προσοχή στον καθορισμό των πεδίων `tag=` ώστε να είναι σωστά. Κάποια tags είναι έγκυρα μόνο για συγκεκριμένες συλλογές αρχείων. Αν καθορίσετε λανθασμένο tag (ή κάνετε ορθογραφικό λάθος) το CVSup θα σβήσει αρχεία τα οποία πιθανώς δεν θέλετε να σβηστούν. Ειδικότερα, για την συλλογή των `ports-*`, χρησιμοποιήστε _ μόνο το_ `tag=.`.

  Το πεδίο `tag=` δείχνει προς ένα συμβολικό tag στο repository. Υπάρχουν δύο είδη tags, τα tags εκδόσεων (revision tags) και τα tags κλάδων (branch tags). Ένα revision tag αναφέρεται σε μια συγκεκριμένη έκδοση. Η σημασία του διατηρείται ίδια από τη μια μέρα στην άλλη. Από την άλλη, ένα branch tag, αναφέρεται στην τελευταία έκδοση μια συγκεκριμένης γραμμής ανάπτυξης, σε κάθε χρονική στιγμή. Επειδή ένα branch tag δεν αναφέρεται σε κάποια συγκεκριμένη έκδοση, μπορεί αύριο να σημαίνει κάτι διαφορετικό από ότι σημαίνει σήμερα.

  Στο Ετικέτες (Tags) για το CVS θα βρείτε branch tags τα οποία μπορεί να σας ενδιαφέρουν. Όταν καθορίζετε ένα tag στο αρχείο ρυθμίσεων του CVSup, θα πρέπει πριν από αυτό να βάζετε τη λέξη κλειδί `tag=` (δηλ. το `RELENG_8` θα γίνει `tag=RELENG_8`). Να έχετε υπόψιν σας ότι για την συλλογή των Ports, το `tag=.` είναι το μόνο έγκυρο.

  Να είστε ιδιαίτερα προσεκτικός, ώστε να γράψετε το tag ακριβώς όπως φαίνεται. Το CVSup δεν μπορεί να διαχωρίσει μεταξύ έγκυρων και μη-έγκυρων tags. Αν γράψετε λάθος το tag, το CVSup θα συμπεριφερθεί σαν να έχετε δώσει ένα έγκυρο tag το οποίο δεν αναφέρεται σε κανένα αρχείο. Στην περίπτωση αυτή θα διαγράψει τα υπάρχοντα αρχεία σας πηγαίου κώδικα.

  Όταν καθορίσετε κάποιο branch tag, φυσιολογικά θα λάβετε τις τελευταίες εκδόσεις των αρχείων που υπάρχουν σε αυτή τη γραμμή ανάπτυξης. Αν θέλετε να λάβετε κάποιες παλιότερες εκδόσεις, μπορείτε να το κάνετε καθορίζοντας μια ημερομηνία μέσω του πεδίου τιμών `date=`. Η σελίδα manual csup(1) εξηγεί πως μπορείτε να το κάνετε.

  Στο παράδειγμα μας, επιθυμούμε να λάβουμε το FreeBSD-CURRENT. Προσθέτουμε τη γραμμή

αυτή στην αρχή του supfile αρχείου μας:

```
*default tag=.
```

Υπάρχει μια σημαντική ειδική περίπτωση όταν δεν καθορίσετε ούτε πεδίο `tag=` ούτε πεδίο `date=`. Στην περίπτωση αυτή θα λάβετε τα κανονικά αρχεία RCS απευθείας από το CVS repository του εξυπηρετητή, αντί για να λάβετε κάποια συγκεκριμένη έκδοση. Οι προγραμματιστές γενικά προτιμούν αυτό τον τρόπο λειτουργίας. Διατηρώντας πλήρες αντίγραφο του CVS repository στα συστήματα τους έχουν την ικανότητα να βλέπουν το ιστορικό αλλαγών κάθε έκδοσης και να εξετάζουν παλιότερες εκδόσεις των αρχείων. Τα παραπάνω πλεονεκτήματα ωστόσο έχουν το κόστος της μεγαλύτερης χρήσης χώρου στο σκληρό δίσκο.

- Από που θέλετε να τα λάβετε;

  Χρησιμοποιούμε το πεδίο `host=` για να πούμε στο `cvsup` από που να λάβει τις ανανεώσεις του. Οποιοδήποτε από τα CVSup mirror sites είναι κατάλληλο, αν και θα πρέπει να προσπαθήσετε να επιλέξετε κάποιο το οποίο να βρίσκεται κοντά σας. Στο παράδειγμα μας, θα χρησιμοποιήσουμε μια φανταστική τοποθεσία διανομής του FreeBSD, το `cvsup99.FreeBSD.org`:

  ```
  *default host=cvsup99.FreeBSD.org
  ```

  Θα πρέπει να αλλάξετε το host σε κάποιο που πραγματικά υπάρχει πριν εκτελέσετε το CVSup. Κάθε φορά που εκτελείτε το `cvsup`, έχετε την δυνατότητα να ανατρέπετε αυτή τη ρύθμιση μέσω της γραμμής εντολών με την επιλογή `-h hostname`.

- Που θέλετε να τα αποθηκεύσετε στο μηχάνημα σας;

  Το πεδίο `prefix=` δηλώνει στην `cvsup` που να αποθηκεύσει τα αρχεία που λαμβάνει. Στο παράδειγμα μας, θα βάλουμε τα αρχεία του πηγαίου κώδικα, απευθείας στο κύριο δέντρο πηγαίου κώδικα, /usr/src. Ο κατάλογος src θεωρείται δεδομένος για τις συλλογές που έχουμε επιλέξει να λάβουμε, και έτσι ο σωστός προσδιορισμός είναι αυτός που φαίνεται παρακάτω:

  ```
  *default prefix=/usr
  ```

- Που θα αποθηκεύσει το `cvsup` τα αρχεία κατάστασης του;

  Ο πελάτης CVSup διατηρεί κάποια αρχεία κατάστασης (status files) σε αυτό που αποκαλείται κατάλογος "base". Τα αρχεία αυτά βοηθούν το CVSup να λειτουργεί πιο αποδοτικά κρατώντας λογαριασμό των ανανεώσεων που έχετε ήδη λάβει. Θα χρησιμοποιήσουμε τον προεπιλεγμένο κατάλογο base, /var/db:

  ```
  *default base=/var/db
  ```

  Αν ο base κατάλογος σας δεν υπάρχει ήδη, τώρα είναι μια καλή στιγμή να τον δημιουργήσετε. Ο πελάτης `cvsup` δεν θα εκτελείται αν ο base κατάλογος δεν υπάρχει.

- Διάφορες ρυθμίσεις για το supfile:

  Υπάρχει ακόμα μια κοινή γραμμή ρυθμίσεων, η οποία τυπικά υπάρχει στο supfile:

  ```
  *default release=cvs delete use-rel-suffix compress
  ```

  Το `release=cvs` δείχνει ότι ο εξυπηρετητής θα πρέπει να λάβει τις πληροφορίες του μέσω του κύριου CVS repository του FreeBSD. Αυτό ισχύει σχεδόν πάντα, αλλά υπάρχουν και άλλες πιθανότητες που ξεφεύγουν από το σκοπό αυτής της συζήτησης.

  Η λέξη `delete` δίνει δικαιώματα στο CVSup να διαγράφει αρχεία. Θα πρέπει πάντοτε να έχετε την επιλογή αυτή, ώστε το CVSup να μπορεί να κρατήσει το δέντρο του πηγαίου σας κώδικα πλήρως ανανεωμένο. Το CVSup είναι αρκετά προσεκτικό ώστε να σβήνει μόνο τα αρχεία που βρίσκονται υπό την ευθύνη του. Αν τυχόν βάλετε έξτρα αρχεία στον ίδιο κατάλογο, δεν θα τα αγγίξει.

  Η επιλογή `use-rel-suffix` είναι... αρχαιολογική. Αν πραγματικά θέλετε να μάθετε σχετικά με αυτήν, διαβάστε τη σελίδα manual cvsup(1). Αλλιώς, απλώς χρησιμοποιήστε την, και μην ανησυχείτε ιδιαίτερα για αυτή.

  Η επιλογή `compress` ενεργοποιεί τη χρήση συμπίεσης τύπου gzip στο κανάλι επικοινωνίας. Αν έχετε σύνδεση δικτύου τύπου T1 ή και πιο γρήγορη, μάλλον δεν θα πρέπει να χρησιμοποιήσετε συμπίεση. Σε διαφορετική περίπτωση, θα βοηθήσει εξαιρετικά.

- Όλες οι επιλογές μαζί:

  Εδώ είναι το πλήρες supfile για το παράδειγμα μας:

  ```
  *default tag=.
  *default host=cvsup99.FreeBSD.org
  *default prefix=/usr
  *default base=/var/db
  *default release=cvs delete use-rel-suffix compress

  src-all
  ```

61.3.1. Το Αρχείο refuse

Όπως αναφέραμε παραπάνω, το CVSup χρησιμοποιεί *μέθοδο pull*. Βασικά αυτό σημαίνει ότι συνδέεστε στον εξυπηρετητή CVSup, αυτός λέει "Αυτά είναι τα αρχεία που μπορείτε να κατεβάσετε από μένα..", και το δικό σας πρόγραμμα απαντάει "Εντάξει, θα πάρω αυτό, αυτό, αυτό, και αυτό." Στην προεπιλεγμένη ρύθμιση, ο πελάτης CVSup θα πάρει κάθε αρχείο που συνδέεται με την συλλογή και το tag που έχετε καθορίσει στο αρχείο ρυθμίσεων. Ωστόσο μπορεί να μην το επιθυμείτε αυτό πάντα, ειδικά αν συγχρονίζετε τα δέντρα doc, ports ή www - οι περισσότεροι άνθρωποι δεν μπορούν να διαβάσουν τέσσερις ή πέντε γλώσσες και έτσι δεν χρειάζεται να κατεβάσουν αρχεία που αναφέρονται ειδικά σε αυτές. Αν χρησιμοποιείτε το CVSup για την συλλογή των Ports, μπορείτε να ξεπεράσετε αυτή τη συμπεριφορά καθορίζοντας συγκεκριμένες συλλογές (π.χ. *ports-astrology*, *ports-biology* αντί για *ports-all*). Ωστόσο, επειδή τα δέντρα doc και www δεν διαθέτουν συλλογές χωρισμένες ανά γλώσσα, μπορείτε να χρησιμοποιήσετε ένα από τα βολικά χαρακτηριστικά του

CVSup: το αρχείο refuse.

Το αρχείο refuse ουσιαστικά λέει στο CVSup ότι δεν πρέπει να πάρει κάθε αρχείο από μια συλλογή. Με άλλα λόγια, λέει στον πελάτη να *αρνηθεί* συγκεκριμένα αρχεία που προσφέρει ο εξυπηρετητής. Το αρχείο refuse μπορεί να βρεθεί (ή να δημιουργηθεί αν δεν έχετε ήδη) στο base/sup/. Το *base* καθορίζεται στο supfile. Το δικό μας *base* είναι στο /var/db, το οποίο σημαίνει ότι το προεπιλεγμένο αρχείο refuse θα είναι το /var/db/sup/refuse.

Το αρχείο refuse έχει ιδιαίτερα απλή μορφή. Απλώς περιέχει τα ονόματα των αρχείων και καταλόγων τα οποία δεν επιθυμείτε να κατεβάσετε. Για παράδειγμα, αν δεν μιλάτε γλώσσες εκτός από Αγγλικά και λίγα Γερμανικά, και δεν αισθάνεστε την ανάγκη να διαβάσετε την Γερμανική μετάφραση της τεκμηρίωσης, μπορείτε να βάλετε τα ακόλουθα στο δικό σας αρχείο refuse:

```
doc/bn_*
doc/da_*
doc/de_*
doc/el_*
doc/es_*
doc/fr_*
doc/it_*
doc/ja_*
doc/nl_*
doc/no_*
doc/pl_*
doc/pt_*
doc/ru_*
doc/sr_*
doc/tr_*
doc/zh_*
```

κ.ο.κ. για τις υπόλοιπες γλώσσες (μπορείτε να βρείτε την πλήρη λίστα στο FreeBSD CVS repository).

Με αυτή τη χρήσιμη δυνατότητα, οι χρήστες που έχουν αργή σύνδεση ή πληρώνουν το Internet με χρονοχρέωση ανά λεπτό, θα μπορέσουν να εξοικονομήσουν πολύτιμο χρόνο καθώς δεν θα χρειάζεται πλέον να κατεβάσουν αρχεία που δεν πρόκειται να χρησιμοποιήσουν ποτέ. Για περισσότερες πληροφορίες σχετικά με τα αρχεία refuse και άλλα χρήσιμα χαρακτηριστικά του CVSup, παρακαλούμε διαβάστε την αντίστοιχη σελίδα του manual.

61.4. Εκτελώντας το CVSup

Είστε τώρα έτοιμοι να δοκιμάσετε μια ανανέωση. Η γραμμή εντολής για το σκοπό αυτό είναι ιδιαίτερα απλή:

```
# cvsup supfile
```

όπου το supfile είναι φυσικά το όνομα του αρχείου supfile που μόλις δημιουργήσατε. Υποθέτοντας ότι χρησιμοποιείτε τα X11, η εντολή `cvsup` θα σας εμφανίσει ένα γραφικό παράθυρο με κάποια

πλήκτρα συνηθισμένων λειτουργιών. Πιέστε το πλήκτρο btn[go], και παρακολουθήστε την εκτέλεση.

Καθώς στην περίπτωση μας ανανεώνεται το πραγματικό δέντρο /usr/src, θα χρειαστεί να εκτελέσετε το πρόγραμμα ως `root` ώστε η `cvsup` να έχει τα δικαιώματα που χρειάζεται για να ανανεώσει τα αρχεία σας. Καθώς μόλις έχετε δημιουργήσει το αρχείο ρυθμίσεων, και δεν έχετε ποτέ πριν χρησιμοποιήσει το πρόγραμμα, ίσως αισθάνεστε λίγο άβολα. Υπάρχει εύκολος τρόπος να κάνετε δοκιμαστική εκτέλεση χωρίς να πειράξετε τα πολύτιμα αρχεία σας. Απλώς δημιουργήστε ένα άδειο κατάλογο σε ένα βολικό μέρος, και δώστε το σαν έξτρα παράμετρο στην γραμμή εντολών:

```
# mkdir /var/tmp/dest
# cvsup supfile /var/tmp/dest
```

Ο κατάλογος που καθορίσατε θα χρησιμοποιηθεί ως προορισμός για όλες τις ανανεώσεις αρχείων. Το CVSup θα εξετάσει τα κανονικά αρχεία σας στο /usr/src, αλλά δεν θα τροποποιήσει ούτε θα διαγράψει κανένα από αυτά. Κάθε ανανέωση αρχείου θα γίνει στον κατάλογο /var/tmp/dest/usr/src. Το CVSup όταν εκτελείται με αυτό τον τρόπο αφήνει επίσης ανέπαφα τα αρχεία κατάστασης του στον κατάλογο base. Οι νέες εκδόσεις των αρχείων αυτών θα γραφούν στον καθορισμένο κατάλογο. Αν έχετε απλώς πρόσβαση ανάγνωσης στο /usr/src, δεν χρειάζεστε να είστε καν `root` για να κάνετε αυτή τη δοκιμαστική εκτέλεση.

Αν δεν εκτελείτε τα X11 ή απλώς δεν σας αρέσουν τα γραφικά περιβάλλοντα, μπορείτε να δώσετε κάποιες επιλογές στην γραμμή εντολών όταν εκτελείτε την `cvsup`:

```
# cvsup -g -L 2 supfile
```

Η επιλογή `-g` λέει στο CVSup να μη χρησιμοποιήσει το γραφικό του περιβάλλον. Αυτό γίνεται αυτόματα αν δεν εκτελούνται τα X11, αλλά διαφορετικά θα πρέπει να το καθορίσετε.

Η επιλογή `-L 2` λέει στο CVSup να εμφανίσει όλες τις λεπτομέρειες για όλες τις ανανεώσεις αρχείων που εκτελεί. Υπάρχουν τρία επίπεδα περιγραφής, από το `-L 0` ως το `-L 2`. Η προεπιλογή είναι το 0, που σημαίνει απόλυτη σιωπή εκτός από μηνύματα λάθους.

Υπάρχουν διαθέσιμες αρκετές ακόμα επιλογές. Για μια περιληπτική λίστα, γράψτε `cvsup -H`. Για περισσότερο λεπτομερείς περιγραφές, δείτε τη σελίδα του manual.

Όταν μείνετε ικανοποιημένος από τον τρόπο που γίνονται οι ανανεώσεις, μπορείτε να κανονίσετε την σε τακτά διαστήματα εκτέλεση του CVSup με την χρήση του cron(8). Προφανώς δεν θα πρέπει να αφήσετε το CVSup να χρησιμοποιεί το γραφικό του περιβάλλον όταν το εκτελείτε μέσω του cron(8).

61.5. Συλλογές Αρχείων τουCVSup

Οι συλλογές αρχείων που διατίθενται μέσω του CVSup είναι οργανωμένες ιεραρχικά. Υπάρχουν λίγες μεγάλες συλλογές, και αυτές χωρίζονται σε μικρότερες υπο-συλλογές. Η λήψη μιας μεγάλης συλλογής, ισοδυναμεί με την λήψη κάθε μιας από τις υπο-συλλογές τις. Οι ιεραρχικές σχέσεις μεταξύ των συλλογών, αντικατοπτρίζονται παρακάτω με την χρήση των εσοχών.

Οι πιο συχνά χρησιμοποιούμενες συλλογές είναι η `src-all`, και η `ports-all`. Οι άλλες συλλογές χρησιμοποιούνται μόνο από μικρές ομάδες ανθρώπων για ειδικούς σκοπούς, και κάποια mirror sites μπορεί να μην τις έχουν καθόλου.

`cvs-all release=cvs`

Το κύριο CVS repository του FreeBSD, που περιλαμβάνει και τον κώδικα κρυπτογραφίας.

`distrib release=cvs`

Αρχεία που αναφέρονται στην διανομή και το mirroring του FreeBSD.

`doc-all release=cvs`

Πηγαίος κώδικας για το FreeBSD Handbook και την υπόλοιπη τεκμηρίωση. Δεν περιλαμβάνει αρχεία για το web site του FreeBSD.

`ports-all release=cvs`

Η συλλογή Ports του FreeBSD.

Αν δεν θέλετε να ανανεώσετε όλο το `ports-all` (το πλήρες δέντρο των ports), αλλά να χρησιμοποιήσετε μια από τις υποσυλλογές που φαίνονται παρακάτω, βεβαιωθείτε ότι *πάντα* ανανεώνετε την υποσυλλογή `ports-base`! Όταν κάτι αλλάζει στο σύστημα μεταγλώττισης των ports που αντιπροσωπεύεται από το `ports-base`, είναι πρακτικά βέβαιο ότι οι αλλαγές αυτές πολύ σύντομα θα χρησιμοποιηθούν από "πραγματικά" ports. Έτσι, αν ανανεώνετε μόνο τα "πραγματικά" ports και αυτά χρησιμοποιούν κάποιες από τις νέες δυνατότητες, υπάρχει μεγάλη πιθανότητα η μεταγλώττιση τους να αποτύχει με κάποιο μυστηριώδες μήνυμα λάθους. Το *πρώτο* πράγμα που πρέπει να κάνετε σε αυτή την περίπτωση είναι να βεβαιωθείτε ότι είναι ενημερωμένη η συλλογή σας `ports-base`.

Αν σκοπεύετε να δημιουργήσετε το δικό σας τοπικό αντίγραφο του ports/INDEX, θα *πρέπει* να δεχτείτε τη συλλογή `ports-all` (ολόκληρο το δέντρο των ports). Η δημιουργία του ports/INDEX από μη-πλήρες δέντρο δεν υποστηρίζεται. Δείτε το FAQ.

`ports-accessibility release=cvs`

Λογισμικό για την βοήθεια χρηστών με αναπηρίες.

`ports-arabic release=cvs`

Υποστήριξη Αραβικής Γλώσσας.

`ports-archivers release=cvs`

Εργαλεία αποθήκευσης και συμπίεσης.

`ports-astro release=cvs`

Ports σχετικά με αστρονομία.

`ports-audio release=cvs`

Υποστήριξη ήχου.

`ports-base release=cvs`

Βασικά αρχεία των ports για υποστήριξη του συστήματος μεταγλώττισης. Διάφορα αρχεία που βρίσκονται στους υποκαταλόγους Mk/ και Tools/ του /usr/ports.

Παρακαλούμε δείτε την σημαντική προειδοποίηση παραπάνω: θα πρέπει *πάντοτε* να ενημερώνετε αυτή την υποσυλλογή, όταν ενημερώνετε οποιοδήποτε τμήμα της συλλογής Ports του FreeBSD.

`ports-benchmarks release=cvs`

Προγράμματα μέτρησης απόδοσης (Benchmarks).

`ports-biology release=cvs`

Βιολογία.

`ports-cad release=cvs`

Εργαλεία σχεδίασης με τη βοήθεια υπολογιστή.

`ports-chinese release=cvs`

Υποστήριξη Κινεζικής Γλώσσας.

`ports-comms release=cvs`

Λογισμικό επικοινωνιών.

`ports-converters release=cvs`

Μετατροπείς χαρακτήρων.

`ports-databases release=cvs`

Βάσεις Δεδομένων.

`ports-deskutils release=cvs`

Αντικείμενα που βρίσκονταν συνήθως σε ένα γραφείο πριν την εφεύρεση των υπολογιστών.

`ports-devel release=cvs`

Βοηθητικά προγράμματα για την ανάπτυξη λογισμικού.

`ports-dns release=cvs`

Λογισμικό σχετικό με DNS.

`ports-editors release=cvs`

Συντάκτες κειμένου.

`ports-emulators release=cvs`

Εξομοιωτές άλλων λειτουργικών συστημάτων.

`ports-finance release=cvs`
: Χρηματοοικονομικά προγράμματα.

`ports-ftp release=cvs`
: Προγράμματα FTP (πελάτες και εξυπηρετητές).

`ports-games release=cvs`
: Παιχνίδια.

`ports-german release=cvs`
: Υποστήριξη Γερμανικής γλώσσας.

`ports-graphics release=cvs`
: Εργαλεία γραφικών.

`ports-hebrew release=cvs`
: Υποστήριξη εβραϊκής γλώσσας.

`ports-hungarian release=cvs`
: Υποστήριξη Ουγγαρέζικης γλώσσας.

`ports-irc release=cvs`
: Προγράμματα για το IRC.

`ports-japanese release=cvs`
: Υποστήριξη Ιαπωνικής γλώσσας.

`ports-java release=cvs`
: Εργαλεία για την Java™.

`ports-korean release=cvs`
: Υποστήριξη Κορεατικής γλώσσας.

`ports-lang release=cvs`
: Γλώσσες προγραμματισμού.

`ports-mail release=cvs`
: Προγράμματα ηλεκτρονικού ταχυδρομείου.

`ports-math release=cvs`
: Λογισμικό μαθηματικών υπολογισμών.

`ports-misc release=cvs`
: Διάφορα βοηθητικά προγράμματα.

`ports-multimedia release=cvs`
: Λογισμικό πολυμέσων.

`ports-net release=cvs`

Λογισμικό δικτύων.

`ports-net-im release=cvs`

Λογισμικό άμεσων μηνυμάτων (instant messaging).

`ports-net-mgmt release=cvs`

Λογισμικό διαχείρισης δικτύων.

`ports-net-p2p release=cvs`

Δικτύωση peer-to-peer.

`ports-news release=cvs`

Λογισμικό για το USENET.

`ports-palm release=cvs`

Λογισμικό για την υποστήριξη συσκευών τύπου Palm™.

`ports-polish release=cvs`

Υποστήριξη Πολωνικής γλώσσας.

`ports-ports-mgmt release=cvs`

Εργαλεία για τη διαχείριση πακέτων και ports.

`ports-portuguese release=cvs`

Υποστήριξη Πορτογαλικής γλώσσας.

`ports-print release=cvs`

Λογισμικό εκτυπώσεων.

`ports-russian release=cvs`

Υποστήριξη Ρωσικής γλώσσας.

`ports-science release=cvs`

Επιστημονικά προγράμματα.

`ports-security release=cvs`

Εργαλεία ασφαλείας.

`ports-shells release=cvs`

Shells για την γραμμή εντολών.

`ports-sysutils release=cvs`

Βοηθητικά προγράμματα συστήματος.

`ports-textproc release=cvs`

Εργαλεία επεξεργασίας κειμένου (δεν περιλαμβάνει επιτραπέζια τυπογραφία).

`ports-ukrainian release=cvs`
: Υποστήριξη Ουκρανικής γλώσσας.

`ports-vietnamese release=cvs`
: Υποστήριξη Βιετναμέζικης γλώσσας.

`ports-www release=cvs`
: Λογισμικό που σχετίζεται με τον παγκόσμιο ιστό (World Wide Web).

`ports-x11 release=cvs`
: Ports για υποστήριξη του συστήματος X Windows.

`ports-x11-clocks release=cvs`
: Ρολόγια για το X11.

`ports-x11-drivers release=cvs`
: Προγράμματα οδήγησης για τα X11.

`ports-x11-fm release=cvs`
: Διαχειριστές αρχείων για τα X11.

`ports-x11-fonts release=cvs`
: Γραμματοσειρές και εργαλεία γραμματοσειρών για X11.

`ports-x11-toolkits release=cvs`
: Εργαλειοθήκες X11.

`ports-x11-servers release=cvs`
: Εξυπηρετητές X11.

`ports-x11-themes release=cvs`
: Θέματα για X11.

`ports-x11-wm release=cvs`
: Διαχειριστές παραθύρων (window managers) για X11.

`projects-all release=cvs`
: Πηγαίος κώδικας για το projects repository του FreeBSD.

`src-all release=cvs`
: Ο βασικός πηγαίος κώδικα του FreeBSD, συμπεριλαμβανομένου του κώδικα κρυπτογραφίας.

`src-base release=cvs`
: Διάφορα αρχεία στην κορυφή του /usr/src.

`src-bin release=cvs`
: Εργαλεία που πιθανόν να απαιτούνται σε κατάσταση λειτουργίας ενός χρήστη (single-user) (/usr/src/bin).

`src-cddl release=cvs`

Εργαλεία και βιβλιοθήκες που καλύπτονται από την άδεια χρήσης CDDL (/usr/src/cddl).

`src-contrib release=cvs`

Εργαλεία και βιβλιοθήκες που δεν ανήκουν στο FreeBSD Project, και τα οποία χρησιμοποιούνται ουσιαστικά αναλλοίωτα (/usr/src/contrib).

`src-crypto release=cvs`

Εργαλεία και βιβλιοθήκες κρυπτογράφησης που δεν ανήκουν στο FreeBSD project και τα οποία χρησιμοποιούνται ουσιαστικά αναλλοίωτα (/usr/src/crypto).

`src-eBones release=cvs`

Kerberos και DES (/usr/src/eBones). Δεν χρησιμοποιούνται στις τρέχουσες εκδόσεις του FreeBSD.

`src-etc release=cvs`

Αρχεία ρυθμίσεων του συστήματος (/usr/src/etc).

`src-games release=cvs`

Παιχνίδια (/usr/src/games).

`src-gnu release=cvs`

Εργαλεία που καλύπτονται από την άδεια χρήσης GNU Public License (/usr/src/gnu).

`src-include release=cvs`

Αρχεία επικεφαλίδων (/usr/src/include).

`src-kerberos5 release=cvs`

Πακέτο ασφαλείας Kerberos5 (/usr/src/kerberos5).

`src-kerberosIV release=cvs`

Πακέτο ασφαλείας KerberosIV (/usr/src/kerberosIV).

`src-lib release=cvs`

Βιβλιοθήκες (/usr/src/lib).

`src-libexec release=cvs`

Προγράμματα συστήματος τα οποία φυσιολογικά εκτελούνται από άλλα προγράμματα (/usr/src/libexec).

`src-release release=cvs`

Αρχεία που απαιτούνται για την παραγωγή μιας έκδοσης του FreeBSD (/usr/src/release).

`src-rescue release=cvs`

Προγράμματα με στατική μεταγλώττιση για χρήση σε έκτακτες περιπτώσεις επαναφοράς του συστήματος. Δείτε το rescue(8) (/usr/src/rescue).

`src-sbin release=cvs`

Εργαλεία συστήματος για λειτουργία σε κατάσταση ενός χρήστη (single user mode) (/usr/src/sbin).

`src-secure release=cvs`

Βιβλιοθήκες και εντολές κρυπτογράφησης (/usr/src/secure).

`src-share release=cvs`

Αρχεία τα οποία μπορεί να είναι κοινά ανάμεσα σε πολλαπλά συστήματα (/usr/src/share).

`src-sys release=cvs`

Ο πυρήνας (/usr/src/sys).

`src-sys-crypto release=cvs`

Κώδικας κρυπτογραφίας του πυρήνα (/usr/src/sys/crypto).

`src-tools release=cvs`

Διάφορα εργαλεία για τη συντήρηση του FreeBSD (/usr/src/tools).

`src-usrbin release=cvs`

Εργαλεία χρήστη (/usr/src/usr.bin).

`src-usrsbin release=cvs`

Εργαλεία συστήματος (/usr/src/usr.sbin).

`www release=cvs`

Ο πηγαίος κώδικας για την τοποθεσία WWW του FreeBSD.

`distrib release=self`

Τα αρχεία ρυθμίσεων του ίδιου του εξυπηρετητή CVSup. Χρησιμοποιείται από CVSup mirror sites.

`gnats release=current`

Η βάση δεδομένων του συστήματος παρακολούθησης προβλημάτων GNATS.

`mail-archive release=current`

Τα αρχεία της λίστας ταχυδρομείου του FreeBSD.

`www release=current`

Προ-επεξεργασμένα αρχεία της δικτυακής τοποθεσίας (WWW) του FreeBSD (όχι ο πηγαίος κώδικας). Χρησιμοποιείται από WWW mirror sites.

61.6. Για Περισσότερες Πληροφορίες

Για το FAQ του CVSup και άλλες πληροφορίες σχετικά με αυτό, δείτε τη Σελίδα του CVSup.

Συζητήσεις σχετικά με τη χρήση του CVSup στο FreeBSD λαμβάνουν χώρα στην ηλεκτρονική λίστα τεχνικών συζητήσεων του FreeBSD. Στη λίστα αυτή, καθώς και στην ηλεκτρονική λίστα

ανακοινώσεων του FreeBSD ανακοινώνονται και οι νέες εκδόσεις του προγράμματος.

Για ερωτήσεις ή αναφορές σφαλμάτων σχετικά με το CVSup ρίξτε μια ματιά στο CVSup FAQ.

61.7. Τοποθεσίες CVSup

Μπορείτε να βρείτε εξυπηρετητές CVSup για το FreeBSD στις ακόλουθες τοποθεσίες:

Chapter 62. Ετικέτες (Tags) για το CVS

Όταν κατεβάζετε ή ανανεώνετε τον πηγαίο κώδικα μέσω της cvs η της CVSup, θα πρέπει να καθορίσετε μια ετικέτα έκδοσης (revision tag). Ένα revision tag αναφέρεται είτε σε μια συγκεκριμένη πορεία ανάπτυξης του FreeBSD, είτε σε ένα συγκεκριμένο χρονικό σημείο. Ο πρώτος τύπος ονομάζεται "ετικέτα κλάδου (branch tag)", και ο δεύτερος ονομάζεται "ετικέτα έκδοσης (release tag)".

62.1. Ετικέτες Κλάδων (Branch Tags)

Όλες αυτές, με την εξαίρεση του `HEAD` (το οποίο είναι πάντα έγκυρη ετικέτα), ισχύουν μόνο για το δέντρο src/. Τα δέντρα ports/, doc/, και www/ δεν έχουν κλάδους.

HEAD

Πρόκειται για το συμβολικό όνομα της κύριας γραμμής ανάπτυξης, ή FreeBSD-CURRENT. Είναι επίσης το προεπιλεγμένο tag αν δεν καθοριστεί κάποιο συγκεκριμένο revision.

Στο CVSup, το tag αυτό αντιπροσωπεύεται από μια `.` (δεν πρόκειται για σημείο στίξης της πρότασης, αλλά για τον πραγματικό χαρακτήρα `.`).

Στο CVS, αυτή είναι και η προεπιλογή αν δεν καθοριστεί revision tag. Συνήθως *δεν* είναι καλή ιδέα να κάνετε checkout και ανανέωση στον πηγαίο κώδικα του CURRENT σε ένα μηχάνημα STABLE, εκτός αν αυτή είναι πραγματικά η πρόθεση σας.

RELENG_9

Η γραμμή ανάπτυξης για το FreeBSD-9.X, γνωστή επίσης και ως FreeBSD 9-STABLE

RELENG_9_0

Η γραμμή έκδοσης του FreeBSD-9.0, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_8

Η γραμμή ανάπτυξης για το FreeBSD-8.X, γνωστή επίσης και ως FreeBSD 8-STABLE

RELENG_8_3

Η γραμμή έκδοσης του FreeBSD-8.3, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_8_2

Η γραμμή έκδοσης του FreeBSD-8.2, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_8_1

Η γραμμή έκδοσης του FreeBSD-8.1, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_8_0

Η γραμμή έκδοσης του FreeBSD-8.0, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_7

Η γραμμή ανάπτυξης για το FreeBSD-7.X, γνωστή επίσης και ως FreeBSD 7-STABLE

RELENG_7_4

Η γραμμή έκδοσης του FreeBSD-7.4, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_7_3

Η γραμμή έκδοσης του FreeBSD-7.3, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_7_2

Η γραμμή έκδοσης του FreeBSD-7.2, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_7_1

Η γραμμή έκδοσης του FreeBSD-7.1, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_7_0

Η γραμμή έκδοσης του FreeBSD-7.0, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_6

Η γραμμή ανάπτυξης για το FreeBSD-6.X, γνωστή επίσης και ως FreeBSD 6-STABLE

RELENG_6_4

Η γραμμή έκδοσης του FreeBSD-6.4, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_6_3

Η γραμμή έκδοσης του FreeBSD-6.3, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_6_2

Η γραμμή έκδοσης του FreeBSD-6.2, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_6_1

Η γραμμή έκδοσης του FreeBSD-6.1, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_6_0

Η γραμμή έκδοσης του FreeBSD-6.0, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες

κρίσιμες διορθώσεις.

RELENG_5

Η γραμμή ανάπτυξης για το FreeBSD-5.X, γνωστή επίσης ως FreeBSD 5-STABLE.

RELENG_5_5

Η γραμμή έκδοσης του FreeBSD-5.5, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_5_4

Η γραμμή έκδοσης του FreeBSD-5.4, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_5_3

Η γραμμή έκδοσης του FreeBSD-5.3, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_5_2

Η γραμμή έκδοσης FreeBSD-5.2 και FreeBSD-5.2.1, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_5_1

Η γραμμή έκδοσης για το FreeBSD-5.1, χρησιμοποιείται μόνο για για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_5_0

Η γραμμή έκδοσης για το FreeBSD-5.0, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4

Η γραμμή ανάπτυξης για το FreeBSD-4.X, γνωστή επίσης και ως FreeBSD 4-STABLE.

RELENG_4_11

Η γραμμή έκδοσης για το FreeBSD-4.11, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_10

Η γραμμή έκδοσης για το FreeBSD-4.10, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_9

Η γραμμή έκδοσης για το FreeBSD-4.9, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_8

Η γραμμή έκδοσης για το FreeBSD-4.8, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_7

Η γραμμή έκδοσης για το FreeBSD-4.7, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_6

Η γραμμή έκδοσης για τα FreeBSD-4.6 και FreeBSD-4.6.2, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_5

Η γραμμή έκδοσης για το FreeBSD-4.5, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_4

Η γραμμή έκδοσης για το FreeBSD-4.4, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_4_3

Η γραμμή έκδοσης για το FreeBSD-4.3, χρησιμοποιείται μόνο για ενημερώσεις ασφαλείας και άλλες κρίσιμες διορθώσεις.

RELENG_3

Η γραμμή ανάπτυξης για το FreeBSD-3.X, γνωστή επίσης και ως 3.X-STABLE.

RELENG_2_2

Η γραμμή ανάπτυξης για το FreeBSD-2.2.X, γνωστή επίσης και ως 2.2-STABLE. Η γραμμή αυτή θεωρείται ουσιαστικά παρωχημένη.

62.2. Ετικέτες Εκδόσεων (Release Tags)

Οι ετικέτες αυτές αναφέρονται σε μια συγκεκριμένη χρονική στιγμή κατά την οποία έγινε μια κανονική έκδοση (release) του FreeBSD. Η διαδικασία της έκδοσης τεκμηριώνεται με περισσότερες λεπτομέρειες στα έγγραφα Πληροφορίες Διαδικασίας Έκδοσης και Διαδικασία Έκδοσης. Το δέντρο src χρησιμοποιεί ονόματα ετικετών που ξεκινούν με τη λέξη `RELENG_`. Τα δέντρα ports και doc χρησιμοποιούν ετικέτες που ξεκινούν με τη λέξη `RELEASE`. Τέλος, στο δέντρο www δεν δίνεται κάποια ειδική ετικέτα που να έχει σχέση με τις εκδόσεις.

RELENG_9_0_0_RELEASE

FreeBSD 9.0

RELENG_8_3_0_RELEASE

FreeBSD 8.3

RELENG_8_2_0_RELEASE

FreeBSD 8.2

RELENG_8_1_0_RELEASE

FreeBSD 8.1

RELENG_8_0_0_RELEASE
FreeBSD 8.0

RELENG_7_4_0_RELEASE
FreeBSD 7.4

RELENG_7_3_0_RELEASE
FreeBSD 7.3

RELENG_7_2_0_RELEASE
FreeBSD 7.2

RELENG_7_1_0_RELEASE
FreeBSD 7.1

RELENG_7_0_0_RELEASE
FreeBSD 7.0

RELENG_6_4_0_RELEASE
FreeBSD 6.4

RELENG_6_3_0_RELEASE
FreeBSD 6.3

RELENG_6_2_0_RELEASE
FreeBSD 6.2

RELENG_6_1_0_RELEASE
FreeBSD 6.1

RELENG_6_0_0_RELEASE
FreeBSD 6.0

RELENG_5_5_0_RELEASE
FreeBSD 5.5

RELENG_5_4_0_RELEASE
FreeBSD 5.4

RELENG_4_11_0_RELEASE
FreeBSD 4.11

RELENG_5_3_0_RELEASE
FreeBSD 5.3

RELENG_4_10_0_RELEASE
FreeBSD 4.10

RELENG_5_2_1_RELEASE
FreeBSD 5.2.1

RELENG_5_2_0_RELEASE
FreeBSD 5.2

RELENG_4_9_0_RELEASE
FreeBSD 4.9

RELENG_5_1_0_RELEASE
FreeBSD 5.1

RELENG_4_8_0_RELEASE
FreeBSD 4.8

RELENG_5_0_0_RELEASE
FreeBSD 5.0

RELENG_4_7_0_RELEASE
FreeBSD 4.7

RELENG_4_6_2_RELEASE
FreeBSD 4.6.2

RELENG_4_6_1_RELEASE
FreeBSD 4.6.1

RELENG_4_6_0_RELEASE
FreeBSD 4.6

RELENG_4_5_0_RELEASE
FreeBSD 4.5

RELENG_4_4_0_RELEASE
FreeBSD 4.4

RELENG_4_3_0_RELEASE
FreeBSD 4.3

RELENG_4_2_0_RELEASE
FreeBSD 4.2

RELENG_4_1_1_RELEASE
FreeBSD 4.1.1

RELENG_4_1_0_RELEASE
FreeBSD 4.1

RELENG_4_0_0_RELEASE
: FreeBSD 4.0

RELENG_3_5_0_RELEASE
: FreeBSD-3.5

RELENG_3_4_0_RELEASE
: FreeBSD-3.4

RELENG_3_3_0_RELEASE
: FreeBSD-3.3

RELENG_3_2_0_RELEASE
: FreeBSD-3.2

RELENG_3_1_0_RELEASE
: FreeBSD-3.1

RELENG_3_0_0_RELEASE
: FreeBSD-3.0

RELENG_2_2_8_RELEASE
: FreeBSD-2.2.8

RELENG_2_2_7_RELEASE
: FreeBSD-2.2.7

RELENG_2_2_6_RELEASE
: FreeBSD-2.2.6

RELENG_2_2_5_RELEASE
: FreeBSD-2.2.5

RELENG_2_2_2_RELEASE
: FreeBSD-2.2.2

RELENG_2_2_1_RELEASE
: FreeBSD-2.2.1

RELENG_2_2_0_RELEASE
: FreeBSD-2.2.0

Chapter 63. Τοποθεσίες AFS

Εξυπηρετητές AFS για το FreeBSD θα βρείτε στις ακόλουθες τοποθεσίες:

Σουηδία

Η διαδρομή για τα αρχεία είναι: /afs/stacken.kth.se/ftp/pub/FreeBSD/

```
stacken.kth.se          # Stacken Computer Club, KTH, Sweden
130.237.234.43          #hot.stacken.kth.se
130.237.237.230         #fishburger.stacken.kth.se
130.237.234.3           #milko.stacken.kth.se
```

Υπεύθυνος Συντήρησης: ftp@stacken.kth.se

Chapter 64. Τοποθεσίες rsync

Το FreeBSD είναι διαθέσιμο μέσω του πρωτοκόλλου rsync στις ακόλουθες τοποθεσίες. Το βοηθητικό πρόγραμμα rsync λειτουργεί με περίπου τον ίδιο τρόπο με την εντολή rcp(1), αλλά έχει περισσότερες επιλογές και χρησιμοποιεί το πρωτόκολλο απομακρυσμένης ανανέωσης το οποίο μεταφέρει μόνο τις διαφορές μεταξύ δύο σετ αρχείων, επιταχύνοντας έτσι ιδιαίτερα το συγχρονισμό μέσω του δικτύου. Αυτό είναι περισσότερο χρήσιμο αν διατηρείτε mirror του διακομιστή FTP ή του CVS Repository του FreeBSD. Η συλλογή εφαρμογών rsync διατίθεται για πολλά λειτουργικά συστήματα, στο FreeBSD δείτε το port net/rsync ή χρησιμοποιήστε το αντίστοιχο πακέτο.

Δημοκρατία της Τσεχίας

rsync://ftp.cz.FreeBSD.org/

Διαθέσιμες Συλλογές:

- ftp: Μερικό mirror του διακομιστή FTP του FreeBSD.
- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD.

Ολλανδία

rsync://ftp.nl.FreeBSD.org/

Διαθέσιμες Συλλογές:

- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD.

Ρωσία

rsync://ftp.mtu.ru/

Διαθέσιμες Συλλογές:

- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD.
- FreeBSD-gnats: Η βάση δεδομένων του συστήματος παρακολούθησης σφαλμάτων GNATS.
- FreeBSD-Archive: Mirror του διακομιστή FTP παλαιότερων εκδόσεων (archive) του FreeBSD.

Σουηδία

rsync://ftp4.se.freebsd.org/

Διαθέσιμες Συλλογές:

- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD

Ταϊβάν

rsync://ftp.tw.FreeBSD.org/

rsync://ftp2.tw.FreeBSD.org/

rsync://ftp6.tw.FreeBSD.org/

Διαθέσιμες Συλλογές:

- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD.

Ηνωμένο Βασίλειο

rsync://rsync.mirrorservice.org/

Διαθέσιμες Συλλογές:

- sites/ftp.freebsd.org: Πλήρες mirror του διακομιστή FTP του FreeBSD.

Ηνωμένες Πολιτείες Αμερικής

rsync://ftp-master.FreeBSD.org/

Ο διακομιστής αυτός μπορεί να χρησιμοποιηθεί μόνο από κύρια mirror sites του FreeBSD.

Διαθέσιμες Συλλογές:

- FreeBSD: Το κύριο (master) σύστημα αρχείων του διακομιστή FTP του FreeBSD.
- acl: Η κύρια λίστα ACL του FreeBSD.

  rsync://ftp13.FreeBSD.org/

  Διαθέσιμες Συλλογές:

- FreeBSD: Πλήρες mirror του διακομιστή FTP του FreeBSD.

Appendix B: Βιβλιογραφία

Αν και τα manual pages παρέχουν μία επίσημη αναφορά για τα διάφορα τμήματα του λειτουργικού συστήματος FreeBSD, δεν εξηγούν πως όλα αυτά ενώνονται μεταξύ τους ώστε το λειτουργικό σύστημα να λειτουργεί ομαλά. Για αυτές τις πληροφορίες, θα πρέπει να συμβουλευτείτε ένα καλό βιβλίο διαχείρισης συστημάτων UNIX® και ένα καλό εγχειρίδιο χρήστη.

B.1. Βιβλία & Περιοδικά σχετικά με το FreeBSD

Διεθνή βιβλία & περιοδικά:

- Using FreeBSD (σε Παραδοσιακά Κινέζικα).
- FreeBSD Unleashed (Μετάφραση σε Απλοποιημένα Κινέζικα), εκδόθηκε από την China Machine Press. ISBN 7-111-10201-0.
- FreeBSD From Scratch Second Edition (σε Απλοποιημένα Κινέζικα), εκδόθηκε από την China Machine Press. ISBN 7-111-10286-X.
- FreeBSD Handbook Second Edition (Μετάφραση σε Απλοποιημένα Κινέζικα), εκδόθηκε από την Posts & Telecom Press. ISBN 7-115-10541-3.
- FreeBSD & Windows (σε Απλοποιημένα Κινέζικα), εκδόθηκε από την China Railway Publishing House. ISBN 7-113-03845-X
- FreeBSD Internet Services HOWTO (σε Απλοποιημένα Κινέζικα), εκδόθηκε από την China Railway Publishing House. ISBN 7-113-03423-3
- FreeBSD (στα Γιαπωνέζικα), εκδόθηκε από την CUTT. ISBN 4-906391-22-2 C3055 P2400E.
- Complete Introduction to FreeBSD (στα Γιαπωνέζικα), εκδόθηκε από την Shoeisha Co., Ltd. ISBN 4-88135-473-6 P3600E.
- Personal UNIX Starter Kit FreeBSD (στα Γιαπωνέζικα), εκδόθηκε από την ASCII. ISBN 4-7561-1733-3 P3000E.
- FreeBSD Handbook (Γιαπωνέζικη μετάφραση), εκδόθηκε από την ASCII. ISBN 4-7561-1580-2 P3800E.
- FreeBSD mit Methode (στα Γερμανικά), εκδόθηκε από την Computer und Literatur Verlag/Vertrieb Hanser, 1998. ISBN 3-932311-31-0.
- FreeBSD de Luxe (στα Γερμανικά), εκδόθηκε από την Verlag Modere Industrie, 2003. ISBN 3-8266-1343-0.
- FreeBSD Install and Utilization Manual (στα Γιαπωνέζικα), εκδόθηκε από την Mainichi Communications Inc..
- Onno W Purbo, Dodi Maryanto, Syahrial Hubbany, Widjil Widodo *Building Internet Server with FreeBSD* (στην Ινδονησιακή γλώσσα), εκδόθηκε από την Elex Media Komputindo.
- Absolute BSD: The Ultimate Guide to FreeBSD (Μετάφραση σε Παραδοσιακά Κινέζικα), εκδόθηκε από την GrandTech Press, 2003. ISBN 986-7944-92-5.
- The FreeBSD 6.0 Book (σε Παραδοσιακά Κινέζικα), εκδόθηκε από την Drmaster, 2006. ISBN 9-575-27878-X.

Βιβλία & περιοδικά στην Αγγλική γλώσσα:

- Absolute FreeBSD, 2nd Edition: The Complete Guide to FreeBSD, εκδόθηκε από την No Starch Press, 2007. ISBN: 978-1-59327-151-0
- The Complete FreeBSD, εκδόθηκε από την O'Reilly, 2003. ISBN: 0596005164
- The FreeBSD Corporate Networker's Guide, εκδόθηκε από την Addison-Wesley, 2000. ISBN: 0201704811
- FreeBSD: An Open-Source Operating System for Your Personal Computer, εκδόθηκε από την The Bit Tree Press, 2001. ISBN: 0971204500
- Teach Yourself FreeBSD in 24 Hours, εκδόθηκε από την Sams, 2002. ISBN: 0672324245
- FreeBSD 6 Unleashed, εκδόθηκε από την Sams, 2006. ISBN: 0672328755
- FreeBSD: The Complete Reference, εκδόθηκε από την McGrawHill, 2003. ISBN: 0072224096
- BSD Magazine, εκδίδεται από την Software Press Sp. z o.o. SK. ISSN 1898-9144

B.2. Οδηγοί χρήστη

- Το Ohio State University έγραψε τα Εισαγωγικά μαθήματα UNIX που διατίθενται σε HTML και PostScript.

  Μια Ιταλική μετάφραση αυτού του κειμένου διατίθεται ως μέρος του FreeBSD Italian Documentation Project.

- Jpman Project, Japan FreeBSD Users Group. FreeBSD User's Reference Manual (Japanese translation). Mainichi Communications Inc., 1998. ISBN4-8399-0088-4 P3800E.
- Το Edinburgh University έγραψε ένα Online οδηγό για νέους στο περιβάλλον του UNIX.

B.3. Οδηγοί διαχειριστή

- Jpman Project, Japan FreeBSD Users Group. FreeBSD System Administrator's Manual (Γιαπωνέζικη μετάφραση). Mainichi Communications Inc., 1998. ISBN4-8399-0109-0 P3300E.
- Dreyfus, Emmanuel. Cahiers de l'Admin: BSD 2nd Ed. (στα Γαλλικά), Eyrolles, 2004. ISBN 2-212-11463-X

B.4. Οδηγοί προγραμματιστών

- Computer Systems Research Group, UC Berkeley. *4.4BSD Programmer's Reference Manual*. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-078-3
- Computer Systems Research Group, UC Berkeley. *4.4BSD Programmer's Supplementary Documents*. O'Reilly & Associates, Inc., 1994. ISBN 1-56592-079-1
- Harbison, Samuel P. and Steele, Guy L. Jr. *C: A Reference Manual*. 4th ed. Prentice Hall, 1995. ISBN 0-13-326224-3
- Kernighan, Brian and Dennis M. Ritchie. *The C Programming Language*. 2nd Ed. PTR Prentice Hall, 1988. ISBN 0-13-110362-8

- Lehey, Greg. *Porting UNIX Software*. O'Reilly & Associates, Inc., 1995. ISBN 1-56592-126-7
- Plauger, P. J. *The Standard C Library*. Prentice Hall, 1992. ISBN 0-13-131509-9
- Spinellis, Diomidis. Code Reading: The Open Source Perspective. Addison-Wesley, 2003. ISBN 0-201-79940-5
- Spinellis, Diomidis. Code Quality: The Open Source Perspective. Addison-Wesley, 2006. ISBN 0-321-16607-8
- Stevens, W. Richard and Stephen A. Rago. *Advanced Programming in the UNIX Environment*. 2nd Ed. Reading, Mass. : Addison-Wesley, 2005. ISBN 0-201-43307-9
- Stevens, W. Richard. *UNIX Network Programming*. 2nd Ed, PTR Prentice Hall, 1998. ISBN 0-13-490012-X

B.5. Το εσωτερικό του λειτουργικού συστήματος

- Andleigh, Prabhat K. *UNIX System Architecture*. Prentice-Hall, Inc., 1990. ISBN 0-13-949843-5
- Jolitz, William. "Porting UNIX to the 386". *Dr. Dobb's Journal*. January 1991-July 1992.
- Leffler, Samuel J., Marshall Kirk McKusick, Michael J Karels and John Quarterman *The Design and Implementation of the 4.3BSD UNIX Operating System*. Reading, Mass. : Addison-Wesley, 1989. ISBN 0-201-06196-1
- Leffler, Samuel J., Marshall Kirk McKusick, *The Design and Implementation of the 4.3BSD UNIX Operating System: Answer Book*. Reading, Mass. : Addison-Wesley, 1991. ISBN 0-201-54629-9
- McKusick, Marshall Kirk, Keith Bostic, Michael J Karels, and John Quarterman. *The Design and Implementation of the 4.4BSD Operating System*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-54979-4

  (Το κεφάλαιο 2 από αυτό το βιβλίο διατίθεται online ως μέρος του FreeBSD Documentation Project.)

- Marshall Kirk McKusick, George V. Neville-Neil *The Design and Implementation of the FreeBSD Operating System*. Boston, Mass. : Addison-Wesley, 2004. ISBN 0-201-70245-2
- Stevens, W. Richard. *TCP/IP Illustrated, Volume 1: The Protocols*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63346-9
- Schimmel, Curt. *Unix Systems for Modern Architectures*. Reading, Mass. : Addison-Wesley, 1994. ISBN 0-201-63338-8
- Stevens, W. Richard. *TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP and the UNIX Domain Protocols*. Reading, Mass. : Addison-Wesley, 1996. ISBN 0-201-63495-3
- Vahalia, Uresh. *UNIX Internals — The New Frontiers*. Prentice Hall, 1996. ISBN 0-13-101908-2
- Wright, Gary R. and W. Richard Stevens. *TCP/IP Illustrated, Volume 2: The Implementation*. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63354-X

B.6. Αναφορές ασφαλείας

- Cheswick, William R. and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily*

Hacker. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-63357-4

- Garfinkel, Simson. *PGP Pretty Good Privacy* O'Reilly & Associates, Inc., 1995. ISBN 1-56592-098-8

B.7. Αναφορές υλικού

- Anderson, Don and Tom Shanley. *Pentium Processor System Architecture*. 2nd Ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40992-5
- Ferraro, Richard F. *Programmer's Guide to the EGA, VGA, and Super VGA Cards*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-62490-7
- Η Intel Corporation δημοσιεύει τεκμηρίωση για τις CPUs, τα chipsets και πρότυπα στο developer web site, συνήθως ως αρχεία PDF.
- Shanley, Tom. *80486 System Architecture*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40994-1
- Shanley, Tom. *ISA System Architecture*. 3rd ed. Reading, Mass. : Addison-Wesley, 1995. ISBN 0-201-40996-8
- Shanley, Tom. *PCI System Architecture*. 4th ed. Reading, Mass. : Addison-Wesley, 1999. ISBN 0-201-30974-2
- Van Gilluwe, Frank. *The Undocumented PC*, 2nd Ed. Reading, Mass: Addison-Wesley Pub. Co., 1996. ISBN 0-201-47950-8
- Messmer, Hans-Peter. *The Indispensable PC Hardware Book*, 4th Ed. Reading, Mass: Addison-Wesley Pub. Co., 2002. ISBN 0-201-59616-4

B.8. Ιστορία του UNIX®

- Lion, John *Lion's Commentary on UNIX, 6th Ed. With Source Code*. ITP Media Group, 1996. ISBN 1573980137
- Raymond, Eric S. *The New Hacker's Dictionary, 3rd edition*. MIT Press, 1996. ISBN 0-262-68092-0. Γνωστό και ως το Jargon File
- Salus, Peter H. *A quarter century of UNIX*. Addison-Wesley Publishing Company, Inc., 1994. ISBN 0-201-54777-5
- Simon Garfinkel, Daniel Weise, Steven Strassmann. *The UNIX-HATERS Handbook*. IDG Books Worldwide, Inc., 1994. ISBN 1-56884-203-1. Εκτός κυκλοφορίας, αλλά διατίθεται online.
- Don Libes, Sandy Ressler *Life with UNIX* - special edition. Prentice-Hall, Inc., 1989. ISBN 0-13-536657-7
- *The BSD family tree*. http://www.FreeBSD.org/cgi/cvsweb.cgi/src/shared/misc/bsd-family-tree η το /usr/shared/misc/bsd-family-tree σε ένα FreeBSD μηχάνημα.
- *Networked Computer Science Technical Reports Library*. http://www.ncstrl.org/
- *Παλαιές BSD εκδόσεις από το Computer Systems Research group (CSRG)*. http://www.mckusick.com/csrg/: Το 4CD set έχει όλες τις BSD εκδόσεις από την 1BSD μέχρι την 4.4BSD και την 4.4BSD-Lite2 (αλλά όχι την 2.11BSD, δυστυχώς). Το τελευταίο δισκάκι περιέχει επίσης τον τελικό πηγαίο κώδικα συν τα αρχεία SCCS.

Β.9. Περιοδικά και εφημερίδες

- *The C/C++ Users Journal*. R&D Publications Inc. ISSN 1075-2838
- *Sys Admin - The Journal for UNIX System Administrators* Miller Freeman, Inc., ISSN 1061-2688
- *freeX - Das Magazin für Linux - BSD - UNIX* (στα Γερμανικά) Computer- und Literaturverlag GmbH, ISSN 1436-7033

Appendix C: Πηγές Πληροφόρησης στο Διαδίκτυο

Η ραγδαία εξέλιξη του FreeBSD καθιστά τα έντυπα μέσα ανίκανα να ακολουθήσουν τις τελευταίες εξελίξεις. Οι ηλεκτρονικές πηγές είναι ο καλύτερος (αν όχι ο μόνος) τρόπος για να παραμείνετε ενήμερος για τις τελευταίες εξελίξεις. Καθώς το FreeBSD είναι μια εθελοντική προσπάθεια, η κοινότητα των χρηστών λειτουργεί και ως "τμήμα τεχνικής υποστήριξης", με το ηλεκτρονικό ταχυδρομείο, τα web forums, και τα USENET news να είναι οι πλέον αποτελεσματικοί τρόποι για να έλθετε σε επαφή με αυτή την κοινότητα.

Στις παρακάτω ενότητες, θα βρείτε τα σημαντικότερα σημεία επικοινωνίας με την κοινότητα χρηστών του FreeBSD. Αν γνωρίζετε και άλλες πηγές, οι οποίες δεν αναφέρονται εδώ, παρακαλούμε να τις στείλετε στην ηλεκτρονική λίστα ομάδας τεκμηρίωσης του FreeBSD ώστε να ενταχθούν και αυτές.

C.1. Λίστες Ηλεκτρονικού Ταχυδρομείου

Οι λίστες ηλεκτρονικού ταχυδρομείου είναι ο πιο άμεσος τρόπος για να απευθύνετε τις ερωτήσεις σας ή να ανοίξετε μια τεχνική συζήτηση που να απευθύνεται σε κοινό ειδικευμένο στο FreeBSD. Υπάρχει μεγάλη ποικιλία από λίστες, οι οποίες καλύπτουν ευρύ φάσμα θεμάτων του FreeBSD. Κατευθύνοντας τις ερωτήσεις σας στη σωστή λίστα, θα εξασφαλίσετε ταχύτερη και ακριβέστερη απόκριση.

Στο τέλος αυτού του κειμένου θα βρείτε ένα πίνακα με τη θεματολογία της κάθε λίστας. *Παρακαλούμε να τον διαβάσετε πριν αρχίσετε να συμμετέχετε ή να στέλνετε μηνύματα σε οποιαδήποτε λίστα*. Οι περισσότεροι από τους συνδρομητές μας δέχονται καθημερινά εκατοντάδες μηνύματα σχετικά με το FreeBSD. Οι κανόνες που έχουμε καθιερώσει, βοηθάνε να γίνεται σωστή χρήση και να διατηρείται σε υψηλό επίπεδο η αναλογία σήματος προς θόρυβο της κάθε λίστας. Εάν ήμασταν πιο χαλαροί, οι λίστες μας θα έχαναν την αποτελεσματικότητα τους ως μέσο επικοινωνίας για το Project.

Αν θέλετε να δοκιμάσετε την ικανότητα σας να στέλνετε μηνύματα στις λίστες του FreeBSD, στείλτε ένα δοκιμαστικό μήνυμα στην λίστα ηλεκτρονική λίστα του FreeBSD για δοκιμαστικά μηνύματα. Παρακαλούμε μη στέλνετε δοκιμαστικά μηνύματα σε οποιαδήποτε άλλη λίστα.

Αν βρίσκεστε σε δίλημμα σχετικά με το ποια λίστα να στείλετε μια ερώτηση, δείτε το Πως να χρησιμοποιείτε με επιτυχία την λίστα ηλεκτρονικού ταχυδρομείου FreeBSD-questions.

Πριν στείλετε κάτι σε οποιαδήποτε λίστα, μάθετε πως να χρησιμοποιείτε καλύτερα τις λίστες ηλεκτρονικού ταχυδρομείου. Για παράδειγμα, δείτε πως μπορείτε να βοηθήσετε ώστε να αποφεύγονται συχνά επαναλαμβανόμενες συζητήσεις, διαβάζοντας το κείμενο Συχνές Ερωτήσεις Σχετικά με τις Λίστες Ταχυδρομείου (FAQ).

Για όλες τις λίστες ηλεκτρονικού ταχυδρομείου διατηρείται αρχείο με τις παλιές δημοσιεύσεις, στο οποίο μπορεί να γίνει αναζήτηση χρησιμοποιώντας την Δικτυακή Τοποθεσία του FreeBSD. Είναι δυνατή η αναζήτηση στο αρχείο μέσω λέξεων-κλειδιών, το οποίο αποτελεί ένα άριστο τρόπο για να

βρείτε απαντήσεις σε συχνές ερωτήσεις. Πριν στείλετε μια ερώτηση, καλό θα είναι να πραγματοποιήσετε μια τέτοια αναζήτηση. Σημειώστε επίσης ότι τα μηνύματα που στέλνονται σε αυτές τις λίστες αποθηκεύονται για πάντα. Αν σας προβληματίζει η προστασία των προσωπικών σας δεδομένων, σας συνιστούμε να χρησιμοποιήσετε μια δευτερεύουσα διεύθυνση email, και να μην γράφετε ποτέ προσωπικές σας πληροφορίες.

C.1.1. Σύνοψη Λιστών

Γενικές λίστες: Οι ακόλουθες είναι γενικές λίστες όπου ο καθένας είναι ελεύθερος (και ενθαρρύνεται) να συμμετέχει:

Λίστα	Σκοπός
freebsd-advocacy	Διαφήμιση και προώθηση του FreeBSD
ηλεκτρονική λίστα ανακοινώσεων του FreeBSD	Σημαντικά γεγονότα και ανακοινώσεις
freebsd-arch	Συζητήσεις αρχιτεκτονικής και σχεδιασμού
freebsd-bugbusters	Συζητήσεις που αναφέρονται στην συντήρηση της βάσης δεδομένων αναφοράς προβλημάτων του FreeBSD, και των σχετικών εργαλείων της
freebsd-bugs	Αναφορές σφαλμάτων
freebsd-chat	Μη-τεχνικά θέματα που σχετίζονται με την κοινότητα του FreeBSD
freebsd-chromium	Θέματα σχετικά με το Chromium στο FreeBSD
ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT	Συζητήσεις που σχετίζονται με τη χρήση FreeBSD-CURRENT
freebsd-isp	Θέματα για Παροχείς Υπηρεσιών Διαδικτύου που χρησιμοποιούν το FreeBSD
freebsd-jobs	Συμβουλευτικές υπηρεσίες και θέσεις εργασίας σχετικές με FreeBSD
freebsd-questions	Απορίες χρηστών και τεχνική υποστήριξη
ηλεκτρονική λίστα Ανακοινώσεων για Θέματα Ασφάλειας του FreeBSD	Ειδοποιήσεις ασφαλείας
ηλεκτρονική λίστα του FreeBSD-STABLE;	Συζητήσεις που σχετίζονται με την χρήση του FreeBSD-STABLE
ηλεκτρονική λίστα του FreeBSD για δοκιμαστικά μηνύματα	Στείλτε εδώ τα δοκιμαστικά σας μηνύματα αντί για μια από τις πραγματικές λίστες

Τεχνικές λίστες: Οι ακόλουθες λίστες είναι για τεχνικές συζητήσεις. Πριν αρχίσετε να συμμετέχετε και να στέλνετε μηνύματα σε αυτές, θα πρέπει να διαβάσετε προσεκτικά την περιγραφή τους. Υπάρχουν αυστηρές οδηγίες για τη χρήση και το περιεχόμενο τους.

Λίστα	Σκοπός
ηλεκτρονική λίστα για ACPI του FreeBSD	Ανάπτυξη της διαχείρισης ενέργειας και του ACPI
freebsd-afs	Μεταφορά του AFS στο FreeBSD
freebsd-aic7xxx	Ανάπτυξη οδηγών για κάρτες Adaptec® AIC 7xxx
freebsd-amd64	Μεταφορά του FreeBSD σε συστήματα AMD64
freebsd-apache	Συζήτηση για ports σχετικά με τον Apache
freebsd-arm	Μεταφορά του FreeBSD σε επεξεργαστές ARM®
freebsd-atm	Χρήση δικτύωσης ATM στο FreeBSD
freebsd-binup	Σχεδίαση και ανάπτυξη του συστήματος έτοιμων ενημερώσεων (binary updates)
freebsd-bluetooth	Χρήση της τεχνολογίας Bluetooth® στο FreeBSD
freebsd-cluster	Χρήση του FreeBSD σε παράλληλα συστήματα
freebsd-cvsweb	Συντήρηση του CVSweb
freebsd-database	Συζήτηση για την χρήση και ανάπτυξη βάσεων δεδομένων στο FreeBSD
freebsd-doc	Δημιουργία τεκμηρίωσης για το FreeBSD
freebsd-desktop	Χρήση και βελτίωση του FreeBSD ως desktop
freebsd-drivers	Δημιουργία οδηγών συσκευών για το FreeBSD
freebsd-eclipse	Συζήτηση για τη χρήση του Eclipse IDE, των εργαλείων του, καθώς και rich client εφαρμογών και ports στο FreeBSD.
freebsd-embedded	Χρήση του FreeBSD σε embedded εφαρμογές
freebsd-eol	Ομότιμη υποστήριξη για λογισμικό σχετικό με FreeBSD, που δεν υποστηρίζεται πλέον από το FreeBSD Project.
freebsd-emulation	Εξομοίωση άλλων συστημάτων, όπως είναι τα Linux/MS-DOS®/Windows®
freebsd-firewire	Τεχνική συζήτηση για FreeBSD FireWire® (iLink, IEEE 1394)
freebsd-fs	Συστήματα αρχείων
freebsd-gecko	Συζήτηση σχετικά με το Gecko Rendering Engine
freebsd-geom	Συζητήσεις σχετικές με το GEOM και τις υλοποιήσεις του
freebsd-gnome	Μεταφορά του GNOME και των εφαρμογών του
freebsd-hackers	Γενικές τεχνικές συζητήσεις

Λίστα	Σκοπός
freebsd-hardware	Γενική συζήτηση για συμβατότητα υλικού με το FreeBSD
freebsd-i18n	Διεθνοποίηση του FreeBSD
freebsd-ia32	Το FreeBSD στην αρχιτεκτονική IA-32 (Intel® x86)
freebsd-ia64	Μεταφορά του FreeBSD στα νέα συστήματα IA64 της Intel®
freebsd-ipfw	Τεχνική συζήτηση που επικεντρώνεται στον επανασχεδιασμό του κώδικα IP του firewall
freebsd-isdn	Ομάδα ανάπτυξης του ISDN
freebsd-jail	Συζήτηση σχετικά με τις δυνατότητες του jail(8)
freebsd-java	Ομάδα ανάπτυξης Java™ και άτομα που μεταφέρουν τα JDK™s στο FreeBSD
freebsd-kde	Μεταφορά του KDE και των εφαρμογών του
freebsd-lfs	Μεταφορά του LFS στο FreeBSD
freebsd-mips	Μεταφορά του FreeBSD σε επεξεργαστές MIPS®
freebsd-mobile	Συζητήσεις σχετικές με φορητά υπολογιστικά συστήματα
freebsd-mono	Εφαρμογές Mono και C# στο FreeBSD
freebsd-mozilla	Μεταφορά του Mozilla στο FreeBSD
ηλεκτρονική λίστα του FreeBSD για τα πολυμέσα	Εφαρμογές πολυμέσων
freebsd-new-bus	Τεχνικές συζητήσεις σχετικές με την αρχιτεκτονική διαύλων
freebsd-net	Συζητήσεις δικτύωσης και πηγαίος κώδικας TCP/IP
freebsd-numerics	Συζητήσεις για υλοποίηση υψηλής ποιότητας συναρτήσεων της βιβλιοθήκης libm
freebsd-office	Εφαρμογές γραφείου στο FreeBSD
freebsd-performance	Ερωτήσεις σχετικές με βελτιστοποίηση απόδοσης για εγκαταστάσεις υψηλής απόδοσης και μεγάλου φορτίου
freebsd-perl	Υποστήριξη ενός αριθμού από ports σχετικά με Perl
freebsd-pf	Συζήτηση και ερωτήσεις σχετικές με το σύστημα packet filter firewall
freebsd-platforms	Συζήτηση για μεταφορά σε μη-Intel® αρχιτεκτονικές

Λίστα	Σκοπός
freebsd-ports	Συζήτηση για την Συλλογή των Ports
freebsd-ports-announce	Σημαντικές ειδήσεις και οδηγίες σχετικές με την Συλλογή των Ports
freebsd-ports-bugs	Συζήτηση για σφάλματα και αναφορές σφαλμάτων (PRs) που αφορούν ports
freebsd-ppc	Μεταφορά του FreeBSD στο PowerPC®
freebsd-proliant	Τεχνική συζήτηση για χρήση του FreeBSD σε διακομιστές HP ProLiant
freebsd-python	Θέματα σχετικά με Python στο FreeBSD
freebsd-rc	Συζήτηση σχετικά με το σύστημα rc.d και την ανάπτυξή του
freebsd-realtime	Ανάπτυξη επεκτάσεων πραγματικού χρόνου του FreeBSD
freebsd-ruby	Συζήτηση σχετικά με τη Ruby στο FreeBSD
freebsd-scsi	Το υποσύστημα SCSI
ηλεκτρονική λίστα του FreeBSD για θέματα ασφάλειας	Θέματα ασφαλείας που επηρεάζουν το FreeBSD
freebsd-small	Χρήση του FreeBSD σε embedded συστήματα (Δεν χρησιμοποιείται πλέον: αντί για αυτή τη λίστα, χρησιμοποιήστε την freebsd-embedded)
freebsd-sparc64	Μεταφορά του FreeBSD σε SPARC® συστήματα
freebsd-standards	Συμμόρφωση του FreeBSD με τα πρότυπα C99 και POSIX®
freebsd-sysinstall	Συζήτηση για την ανάπτυξη του sysinstall(8)
freebsd-threads	Πολυνηματική επεξεργασία στο FreeBSD
freebsd-tilera	Μεταφορά του FreeBSD στην οικογένεια CPU Tilera
freebsd-tokenring	Υποστήριξη του Token Ring στο FreeBSD
freebsd-toolchain	Συντήρηση των εργαλείων του FreeBSD
freebsd-usb	Συζήτηση υποστήριξης του USB στο FreeBSD
freebsd-virtualization	Συζήτηση σχετικά με διάφορες τεχνικές εικονικοποίησης που υποστηρίζονται από το FreeBSD
freebsd-vuxml	Συζήτηση για την υποδομή VuXML
freebsd-x11	Συντήρηση και υποστήριξη του X11 στο FreeBSD
freebsd-xen	Συζήτηση για τη μεταφορά του FreeBSD στο Xen™ - υλοποίηση και χρήση

Λίστα	Σκοπός
freebsd-xfce	XFCE στο FreeBSD - Μεταφορά και συντήρηση
freebsd-zope	Zope στο FreeBSD - Μεταφορά και συντήρηση

Περιορισμένες λίστες: Οι ακόλουθες λίστες είναι για πιο ειδικό (και απαιτητικό) κοινό και πιθανώς δεν ενδιαφέρουν το γενικό κοινό. Πριν αρχίσετε να συμμετέχετε σε κάποια από αυτές, καλό θα είναι να έχετε παρακολουθήσει τις τεχνικές λίστες, ώστε να αντιλαμβάνεστε τον κώδικα επικοινωνίας και συμπεριφοράς που ισχύει σε αυτές.

Λίστα	Σκοπός
freebsd-hubs	Άτομα που διατηρούν mirror sites (υποστήριξη υποδομών)
freebsd-user-groups	Οργάνωση των συλλόγων χρηστών
freebsd-vendors	Οργάνωση μεταπωλητών πριν από επίσημες εκδόσεις
freebsd-wip-status	Κατάσταση εργασιών του FreeBSD που βρίσκονται σε εξέλιξη (Work-in-Progress).
freebsd-wireless	Συζήτηση σχετικά με τη στοίβα 802.11, τα εργαλεία ασύρματου δικτύου και την ανάπτυξη προγραμμάτων οδήγησης.
freebsd-www	Συντηρητές του www.FreeBSD.org

Λίστες digest: Όλες οι παραπάνω λίστες διατίθενται και σε μορφή digest (περίληψης). Μόλις εγγραφείτε σε μία λίστα, μπορείτε να αλλάξετε τις επιλογές digest στο τμήμα ρυθμίσεων του λογαριασμού σας.

Λίστες SVN: Οι ακόλουθες λίστες είναι για όσους ενδιαφέρονται να βλέπουν τα μηνύματα (log) που δείχνουν τις αλλαγές σε διάφορες περιοχές του πηγαίου κώδικα. Είναι λίστες *μόνο για ανάγνωση* και δεν πρέπει να στέλνετε μηνύματα σε αυτές.

Λίστα	Περιοχή πηγαίου κώδικα	Περιγραφή περιοχής (κώδικας για)
svn-doc-all	/usr/doc	Όλες οι αλλαγές στο δέντρο doc του Subversion (εκτός από τις περιοχές user, projects και translations)
svn-doc-head	/usr/doc	Όλες οι αλλαγές στον κλάδο "head" του doc Subversion repository
svn-doc-projects	/usr/doc/projects	Όλες οι αλλαγές στην περιοχή "projects" του doc Subversion repository

Λίστα	Περιοχή πηγαίου κώδικα	Περιγραφή περιοχής (κώδικας για)
svn-doc-svnadmin	/usr/doc	Όλες οι αλλαγές στα scripts διαχείρισης, hooks και άλλα δεδομένα ρυθμίσεων του doc Subversion repository
svn-ports-all	/usr/ports	Όλες οι αλλαγές στο ports Subversion repository
svn-ports-head	/usr/ports	Όλες οι αλλαγές στον κλάδο "head" του ports Subversion repository
svn-ports-svnadmin	/usr/ports	Όλες οι αλλαγές στα scripts διαχείρισης, hooks και άλλα δεδομένα ρυθμίσεων του ports Subversion repository.
ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα του FreeBSD (εξαιρούνται τα δέντρα "user" και "projects")	/usr/src	Όλες οι αλλαγές στο src Subversion repository (εκτός από τις περιοχές user και projects)
ηλεκτρονική λίστα μηνυμάτων SVN commit πηγαίου κώδικα για τον κλάδο head/-current	/usr/src	Όλες οι αλλαγές στον κλάδο "head" του src Subversion repository (πρόκειται για τον κλάδο FreeBSD-CURRENT)
svn-src-projects	/usr/projects	Όλες οι αλλαγές στην περιοχή πηγαίου κώδικα projects του Subversion repository
svn-src-release	/usr/src	Όλες οι αλλαγές στην περιοχή πηγαίου κώδικα releases του Subversion repository
svn-src-releng	/usr/src	Όλες οι αλλαγές σε όλους τους κλάδους πηγαίου κώδικα releng του Subversion repository (πρόκειται για τους κλάδους security / release engineering)
svn-src-stable	/usr/src	Όλες οι αλλαγές σε όλους τους κλάδους πηγαίου κώδικα stable του Subversion repository
svn-src-stable-6	/usr/src	Όλες οι αλλαγές στον κλάδο πηγαίου κώδικα stable/6 του Subversion repository
svn-src-stable-7	/usr/src	Όλες οι αλλαγές στον κλάδο πηγαίου κώδικα stable/7 του Subversion repository

Λίστα	Περιοχή πηγαίου κώδικα	Περιγραφή περιοχής (κώδικας για)
svn-src-stable-8	/usr/src	Όλες οι αλλαγές στον κλάδο πηγαίου κώδικα stable/8 του Subversion repository
ηλεκτρονική λίστα μηνυμάτων SVN commit μόνο για το δέντρο πηγαίου κώδικα 9-stable	/usr/src	Όλες οι αλλαγές στον κλάδο πηγαίου κώδικα stable/9 του Subversion repository
svn-src-stable-other	/usr/src	Όλες οι αλλαγές στους παλιούς stable κλάδους πηγαίου κώδικα του Subversion repository
svn-src-svnadmin	/usr/src	Όλες οι αλλαγές στα scripts διαχείρισης, τα hooks, και άλλα δεδομένα που αφορούν τις ρυθμίσεις του Subversion repository
svn-src-user	/usr/src	Όλες οι αλλαγές στην πειραματική περιοχή πηγαίου κώδικα user του Subversion repository
svn-src-vendor	/usr/src	Όλες οι αλλαγές στην περιοχή εργασίας πηγαίου κώδικα vendor του Subversion repository

C.1.2. Πως να Εγγραφείτε

Για να εγγραφείτε σε μία λίστα, επιλέξτε το όνομα της από τους παραπάνω δεσμούς ή πηγαίνετε στο https://lists.freebsd.org και επιλέξτε την λίστα για την οποία ενδιαφέρεστε. Η σελίδα της λίστας πρέπει να περιέχει όλες τις απαραίτητες πληροφορίες εγγραφής.

Για να γράψετε σε μια λίστα, στείλτε το μήνυμα σας στο όνομα-λίστας@FreeBSD.org. Το μήνυμα σας θα διανεμηθεί σε όλα τα μέλη της λίστας, σε οποιοδήποτε σημείο του κόσμου και αν βρίσκονται.

Για να διαγραφείτε από μια λίστα, επιλέξτε το URL που βρίσκεται στο τέλος κάθε μηνύματος που λαμβάνετε από την λίστα. Μπορείτε επίσης να στείλετε ένα μήνυμα στο όνομα-λίστας-unsubscribe@FreeBSD.org για να διαγραφείτε μόνος σας.

Για ακόμα μια φορά, θα θέλαμε να σας ζητήσουμε να διατηρήσετε τη συζήτηση των τεχνικών λιστών στα αντίστοιχα τεχνικά θέματα. Αν ενδιαφέρεστε μόνο για σημαντικές ανακοινώσεις, τότε προτείνουμε να εγγραφείτε στην ηλεκτρονική λίστα ανακοινώσεων του FreeBSD, η οποία έχει μικρή κίνηση.

C.1.3. Πίνακες Λιστών

Όλες οι FreeBSD λίστες έχουν συγκεκριμένους βασικούς κανόνες οι οποίοι πρέπει να

ακολουθούνται από οποιονδήποτε τις χρησιμοποιεί. Όποιος αποτύχει να ακολουθήσει αυτούς τους κανόνες θα λάβει δύο (2) γραπτές προειδοποιήσεις από τον FreeBSD Postmaster postmaster@FreeBSD.org. Σε περίπτωση τρίτης παραβίασης, το άτομο αυτό θα απομακρυνθεί από όλες τις λίστες του FreeBSD και τα μηνύματα του προς αυτές θα φιλτράρονται. Λυπόμαστε που χρειάζεται να επιβάλλουμε αυτούς τους κανόνες και μέτρα, αλλά το σημερινό Διαδίκτυο είναι καθώς φαίνεται ένα πολύ σκληρό περιβάλλον, και πολλοί δεν εκτιμούν πόσο εύθραυστοι είναι μερικοί μηχανισμοί του.

Κανόνες:

- Το θέμα κάθε μηνύματος πρέπει να είναι σχετικό με τον βασικό σκοπό της λίστας που στάλθηκε, π.χ. αν η λίστα σχετίζεται με τεχνικά θέματα τότε το μήνυμα σας πρέπει να περιέχει τεχνικό περιεχόμενο. Η άσχετη φλυαρία ή το flaming μειώνει την αξία της λίστας για όλους που την παρακολουθούν και δεν μπορούμε να ανεχτούμε αυτή τη συμπεριφορά. Για ελεύθερες συζητήσεις χωρίς κάποιο συγκεκριμένο θέμα, διατίθεται η ηλεκτρονική λίστα γενικών συζητήσεων του FreeBSD την οποία και θα πρέπει να χρησιμοποιείτε.
- Κανένα μήνυμα δεν θα πρέπει να σταλεί σε περισσότερες από 2 λίστες, και σε 2 μόνο όταν υπάρχει ξεκάθαρος και προφανής λόγος για κάτι τέτοιο. Πολλοί συνδρομητές είναι έτσι και αλλιώς γραμμένοι σε περισσότερες από μία λίστες. Έτσι, αν δεν πρόκειται να κάνετε κάποιο περίεργο συνδυασμό (π.χ. "-stable & -scsi"), δεν υπάρχει λόγος να στείλετε μήνυμα σε περισσότερες από μία λίστα κάθε φορά. Αν λάβετε κάποιο μήνυμα στο οποίο φαίνονται πολλαπλές λίστες στην γραμμή `Cc`, καλό θα είναι να περικόψετε κάποιες από αυτές πριν στείλετε απάντηση. *Θεωρείστε υπεύθυνος για τα δικά σας cross-postings, ανεξάρτητα ποιος είναι ο δημιουργός τους.*
- Προσωπικές επιθέσεις και ασέβεια (στο περιεχόμενο μιας αντιπαράθεσης) δεν επιτρέπονται, και αυτό αφορά τόσο τους χρήστες όσο και τους developers. Μεγάλες παραβάσεις των κανόνων (netiquette), όπως χρήση τμημάτων ή ολόκληρων προσωπικών μηνυμάτων όταν δεν έχει δοθεί άδεια για να γίνει αυτό και δεν ήταν αναμενόμενο, αποδοκιμάζονται αλλά δεν απαγορεύονται ρητά. *Όμως*, υπάρχουν μερικές περιπτώσεις όπου τέτοιο περιεχόμενο εμπίπτει στους κανονισμούς κάποιας λίστας και μπορεί να οδηγήσει σε προειδοποίηση (ή ακόμα και αποκλεισμό) από αυτήν.
- Διαφήμιση προϊόντων ή υπηρεσιών που δεν σχετίζονται με το FreeBSD απαγορεύεται αυστηρά και θα οδηγήσει σε άμεσο αποκλεισμό αν είναι φανερό ότι ο πταίστης διαφημίζεται με spam.

Ατομικοί πίνακες λιστών:

ηλεκτρονική λίστα για ACPI του FreeBSD

Ανάπτυξη της διαχείρισης ενέργειας και του ACPI

freebsd-afs

Andrew File System

Αυτή η λίστα είναι για συζήτηση της μεταφοράς και της χρήσης του AFS από το CMU/Transarc

ηλεκτρονική λίστα ανακοινώσεων του FreeBSD

Σημαντικά γεγονότα και ανακοινώσεις

Αυτή η λίστα είναι για άτομα που ενδιαφέρονται μόνο για περιστασιακές ανακοινώσεις

σημαντικών γεγονότων του FreeBSD. Περιλαμβάνει ανακοινώσεις σχετικά με snapshots και άλλα releases. Επίσης δημοσιεύονται σε αυτήν ανακοινώσεις για νέες ικανότητες του FreeBSD. Μπορεί να περιέχει εκκλήσεις για εθελοντές κτλ. Πρόκειται για μία λίστα με μικρή κίνηση, και οι δημοσιεύσεις ελέγχονται αυστηρά.

freebsd-arch

Συζητήσεις αρχιτεκτονικής και σχεδιασμού

Σε αυτή την λίστα συζητείται η αρχιτεκτονική του FreeBSD. Τα μηνύματα είναι κατά κύριο λόγο αρκετά τεχνικά. Παραδείγματα σχετικών θεμάτων είναι:

- Πως να επανασχεδιαστεί το σύστημα μεταγλώττισης ώστε να εκτελεί ταυτόχρονα πολλές προσαρμοσμένες μεταγλωττίσεις.
- Τι πρέπει να επισκευαστεί στο VFS ώστε να λειτουργούν τα Heidemann layers.
- Πώς πρέπει να μετατρέψουμε τη διεπαφή (interface) των οδηγών συσκευών ώστε να μπορούμε να χρησιμοποιήσουμε τα ίδια προγράμματα οδήγησης σε πολλούς διαύλους και αρχιτεκτονικές.
- Πως να γράψετε ένα οδηγό δικτύου.

freebsd-binup

Project αναβάθμισης του FreeBSD μέσω έτοιμων (δυαδικών) αρχείων

Σε αυτή την λίστα συζητείται το σύστημα αναβάθμισης μέσω έτοιμων (binary) αρχείων, ή binup. Σε αυτή τη λίστα ανήκουν θέματα σχεδιασμού, λεπτομέρειες υλοποίησης, "patches", αναφορές σφαλμάτων, αναφορές κατάστασης, αιτήσεις για πρόσθετα χαρακτηριστικά, commit logs, και ότι άλλο σχετίζεται με το binup.

freebsd-bluetooth

Χρήση της τεχνολογίας Bluetooth® στο FreeBSD

Σε αυτή τη λίστα συναθροίζονται οι χρήστες του Bluetooth® στο FreeBSD. Η λίστα ασχολείται με θέματα σχεδιασμού, λεπτομέρειες υλοποίησης, "patches", αναφορές σφαλμάτων, αναφορές κατάστασης, αιτήσεις για πρόσθετα χαρακτηριστικά, και ότι άλλο σχετίζεται με το Bluetooth®.

freebsd-bugbusters

Προσπάθεια οργάνωσης του χειρισμού των αναφορών προβλημάτων

Σκοπός αυτής της λίστας είναι να λειτουργεί ως χώρος οργάνωσης και συζήτησης για τον Bugmeister, τους Bugbusters, και όσους άλλους ενδιαφέρονται για την βάση δεδομένων PR. Αυτή ή λίστα δεν είναι για συζητήσεις σχετικά με ιδιαίτερα σφάλματα, "patches" ή PRs.

freebsd-bugs

Αναφορές σφαλμάτων

Αυτή η λίστα είναι για αναφορές σφαλμάτων του FreeBSD. Όποτε είναι δυνατό, τα σφάλματα πρέπει να στέλνονται με την εντολή send-pr(1) ή μέσω της αντίστοιχης διεπαφή WEB.

freebsd-chat

Μη τεχνικά θέματα που σχετίζονται με την κοινότητα του FreeBSD

Αυτή η λίστα περιέχει κοινωνικές συζητήσεις, και γενικότερα ότι δεν σχετίζεται με τεχνικές πληροφορίες με τις οποίες ασχολούνται οι υπόλοιπες λίστες. Περιέχει συζητήσεις για το αν ο Jordan μοιάζει με μικρό κουνάβι ή όχι, για το αν πρέπει ή όχι να γράφουμε με κεφαλαία, ποιος πίνει πολύ καφέ, που φτιάχνεται η καλύτερη μπύρα, ποιος φτιάχνει μπύρα στο υπόγειο του, και άλλα. Περιστασιακές ανακοινώσεις σημαντικών γεγονότων (όπως πάρτυ, γάμοι, γεννήσεις, καινούργιες δουλειές κλπ) μπορούν να γίνουν στις τεχνικές λίστες, αλλά οι απαντήσεις τους πρέπει να στέλνονται στην λίστα -chat.

freebsd-chromium

Θέματα σχετικά με το Chromium στο FreeBSD

Λίστα συζητήσεων για την υποστήριξη του Chromium στο FreeBSD. Πρόκειται για τεχνική λίστα σχετική με την ανάπτυξη και εγκατάσταση του Chromium. :: *Ομάδα core του FreeBSD*

Αυτή είναι μία εσωτερική λίστα για χρήση από τα μέλη του core. Σε αυτή τη λίστα μπορείτε να στείλετε μηνύματα, όταν προκύψει κάποιο θέμα σχετικό με το FreeBSD το οποίο απαιτεί διαιτησία ή λεπτομερή εξέταση.

ηλεκτρονική λίστα της έκδοσης FreeBSD-CURRENT

Συζητήσεις σχετικά με την χρήση του FreeBSD-CURRENT

Αυτή η λίστα είναι για χρήστες του FreeBSD-CURRENT. Περιέχει προειδοποιήσεις για νέα χαρακτηριστικά που πρόκειται να προστεθούν στο -CURRENT και τα οποία θα επηρεάσουν τους χρήστες, και οδηγίες για τις κινήσεις που πρέπει να γίνουν ώστε να παραμείνετε στο -CURRENT. Όποιος εκτελεί το "CURRENT" πρέπει να εγγραφεί σε αυτήν την λίστα. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-cvsweb

FreeBSD CVSweb Project

Τεχνικές συζητήσεις για την χρήση, την ανάπτυξη και την συντήρηση του FreeBSD-CVSweb.

freebsd-desktop

Χρήση και βελτίωση του FreeBSD ως desktop

Ή λίστα αυτή προορίζεται για συζητήσεις σχετικές με τη χρήση του FreeBSD ως desktop. Απευθύνεται κυρίως σε χρήστες και προγραμματιστές που επιθυμούν να συζητήσουν τα προβλήματα που παρουσιάζει το FreeBSD σε desktop εφαρμογές, καθώς και αντίστοιχες βελτιώσεις.

freebsd-doc

Project τεκμηρίωσης του FreeBSD

Αυτή η λίστα είναι για συζήτηση θεμάτων και projects που σχετίζονται με την δημιουργία τεκμηρίωσης για το FreeBSD. Τα μέλη αυτής της λίστας αποκαλούνται συνολικά ως "The FreeBSD Documentation Project". Είναι μια ανοικτή λίστα και είστε ελεύθερος να συμμετέχετε και να

συνεισφέρετε!

freebsd-drivers

Δημιουργία οδηγών συσκευών για το FreeBSD

Αυτή η λίστα προορίζεται για τεχνικές συζητήσεις σχετικές με οδηγούς συσκευών στο FreeBSD. Χρησιμοποιείται κυρίως από τους δημιουργούς οδηγών συσκευών για ερωτήσεις σχετικές με τη συγγραφή οδηγών, χρησιμοποιώντας τα APIs που παρέχει ο πυρήνας του FreeBSD.

freebsd-eclipse

FreeBSD χρήστες του Eclipse IDE, των εργαλείων του, rich client εφαρμογών, και ports.

Πρόθεση της λίστας αυτής είναι να προσφέρει αμοιβαία υποστήριξη για ότι έχει να κάνει με την επιλογή, εγκατάσταση, χρήση, ανάπτυξη και συντήρηση του Eclipse IDE, των εργαλείων του, εφαρμογών rich client στην πλατφόρμα του FreeBSD και για βοήθεια σχετικά με την μεταφορά του Eclipse IDE και των πρόσθετων του στο περιβάλλον του FreeBSD.

Πρόθεση της είναι επίσης να διευκολύνει την ανταλλαγή πληροφοριών ανάμεσα στην κοινότητα του Eclipse και στην κοινότητα του FreeBSD, προς όφελος και των δύο.

Αν και η λίστα επικεντρώνεται κυρίως στις ανάγκες των χρηστών του Eclipse, προσφέρει επίσης ένα χώρο συζήτησης για όσους θέλουν να αναπτύξουν εφαρμογές σχετικές με το FreeBSD χρησιμοποιώντας το Eclipse.

freebsd-embedded

Χρήση του FreeBSD σε embedded εφαρμογές

Η λίστα συζητά θέματα σχετικά με την χρήση του FreeBSD σε embedded συστήματα. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα. Για τον σκοπό της λίστας αυτής, ορίζουμε ως embedded συστήματα τις υπολογιστικές συσκευές που δεν προορίζονται για desktop εφαρμογές, και που συνήθως καλύπτουν μια μόνο ανάγκη, αντίθετα με τα γενικά υπολογιστικά περιβάλλοντα. Συμπεριλαμβάνονται, εκτός των άλλων, όλα τα τηλέφωνα, δικτυακός εξοπλισμός όπως routers, switches και PBXs, εξοπλισμός μετρήσεων από απόσταση, PDAs, συστήματα Point Of Sale, και πάει λέγοντας.

freebsd-emulation

Εξομοίωση άλλων συστημάτων όπως είναι τα Linux/MS-DOS®/Windows®

Είναι μια λίστα για τεχνικές συζητήσεις, σχετικές με την εκτέλεση στο FreeBSD προγραμμάτων που δημιουργήθηκαν για άλλα λειτουργικά.

freebsd-eol

Ομότιμη υποστήριξη για λογισμικό σχετικό με το FreeBSD που δεν υποστηρίζεται πλέον από το FreeBSD Project.

Αυτή η λίστα είναι για όσους ενδιαφέρονται να παρέχουν ή να χρησιμοποιήσουν την ομότιμη υποστήριξη για λογισμικό σχετικό με το FreeBSD που δεν υποστηρίζεται πλέον από το FreeBSD Project (π.χ., με την μορφή "patches" και ανακοινώσεων ασφαλείας).

freebsd-firewire

FireWire® (iLink, IEEE 1394)

Αυτή η λίστα είναι για την συζήτηση της σχεδίασης και υλοποίησης ενός υποσυστήματος FireWire® (γνωστό και ως IEEE 1394 ή iLink) για το FreeBSD. Σχετικά θέματα είναι τα πρότυπα, οι συσκευές διαύλου και τα πρωτόκολλά τους, κάρτες, προσαρμογείς και chipsets, και η αρχιτεκτονική και η υλοποίηση του κώδικα για την σωστή υποστήριξη τους.

freebsd-fs

Συστήματα αρχείων

Συζητήσεις σχετικές με τα συστήματα αρχείων του FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-gecko

Gecko Rendering Engine

Συζητήσεις σχετικές με εφαρμογές που χρησιμοποιούν την μηχανή Gecko στο FreeBSD.

Η συζήτηση επικεντρώνεται σε εφαρμογές της Συλλογής των Ports που χρησιμοποιούν τη μηχανή Gecko, και ειδικότερα την εγκατάσταση, ανάπτυξη και υποστήριξη τους στο FreeBSD.

freebsd-geom

GEOM

Συζητήσεις σχετικές με το GEOM και παρόμοιες υλοποιήσεις. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-gnome

GNOME

Συζητήσεις σχετικές με το περιβάλλον GNOME για συστήματα FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-ipfw

IP Firewall

Αυτή η λίστα είναι για τεχνικές συζητήσεις που αφορούν τον επανασχεδιασμό του κώδικα IP firewall στο FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-ia64

Μεταφορά του FreeBSD στην αρχιτεκτονική IA64

Πρόκειται για μια τεχνική λίστα, για άτομα που δουλεύουν ενεργά στην μεταφορά του FreeBSD στην πλατφόρμα IA-64 της Intel®, για να αναφέρουν προβλήματα ή να συζητήσουν εναλλακτικές λύσεις. Άτομα που ενδιαφέρονται να παρακολουθήσουν την τεχνική συζήτηση είναι επίσης ευπρόσδεκτα.

freebsd-isdn

Ανάπτυξη του ISDN

Αυτή η λίστα είναι για άτομα που συζητούν την ανάπτυξη της υποστήριξης ISDN στο FreeBSD.

freebsd-java

Ανάπτυξη της Java™

Αυτή η λίστα είναι για άτομα που συζητούν την ανάπτυξη σημαντικών εφαρμογών Java™ για το FreeBSD και την μεταφορά και συντήρηση των JDK™s.

freebsd-jobs

Ζήτηση και προσφορά εργασίας

Αυτός είναι ένας χώρος για δημοσίευση ανακοινώσεων για προσφορά και ζήτηση εργασίας που σχετίζεται με το FreeBSD, καθώς και βιογραφικών σχετικών με το FreeBSD. Αν για παράδειγμα αναζητάτε εργασία σχετική με το FreeBSD, ή προσφέρετε μια θέση εργασίας σχετική με το FreeBSD, αυτό είναι το σωστό μέρος για να τη διαφημίσετε. Η λίστα αυτή *δεν* είναι για γενικά θέματα εργασίας, για τα οποία υπάρχει πληθώρα από άλλες λίστες στο Διαδίκτυο.

Αυτή η λίστα, όπως και οι υπόλοιπες λίστες του FreeBSD.org, διανέμονται παγκόσμια. Έτσι, πρέπει να είστε σαφής για την τοποθεσία και την δυνατότητα τηλεργασίας ή βοήθειας στην μετοίκηση.

Το μήνυμα σας θα πρέπει να χρησιμοποιεί μόνο ανοιχτά πρότυπα - κατά προτίμηση απλό κείμενο, αν και βασικής μορφής Portable Document Format (PDF), HTML, και μερικά άλλα είναι αποδεκτά από πολλούς χρήστες. Κλειστά πρότυπα όπως το Microsoft® Word (.doc) θα απορριφθούν από τον διακομιστή της λίστας.

freebsd-kde

KDE

Συζητήσεις που αφορούν το KDE σε συστήματα FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-hackers

Τεχνικές συζητήσεις

Είναι ένας χώρος για τεχνικές συζητήσεις σχετικές με το FreeBSD. Αυτή είναι η κύρια τεχνική λίστα. Είναι για άτομα που αναπτύσσουν ενεργά το FreeBSD, για να αναφέρουν προβλήματα ή να συζητήσουν εναλλακτικές λύσεις. Άτομα που ενδιαφέρονται να παρακολουθήσουν την τεχνική συζήτηση είναι ευπρόσδεκτα. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-hardware

Γενική συζήτηση για υλικό κι εξαρτήματα υπολογιστών στο FreeBSD

Γενικές συζητήσεις για τύπους υλικού που λειτουργούν στο FreeBSD, διάφορα προβλήματα και προτάσεις σχετικά με το τι να αγοράσετε ή να αποφύγετε.

freebsd-hubs

Mirror sites

Ανακοινώσεις και συζητήσεις για άτομα που συντηρούν mirror sites του FreeBSD.

freebsd-isp

Θέματα για Παροχείς Υπηρεσιών Διαδικτύου

Αυτή η λίστα είναι για συζήτηση θεμάτων σχετικών με Παροχείς Υπηρεσιών Διαδικτύου (ISPs) που χρησιμοποιούν FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-mono

Εφαρμογές Mono και C# στο FreeBSD

Αυτή η λίστα είναι για συζήτηση θεμάτων σχετικών με το σύστημα ανάπτυξης εφαρμογών Mono στο FreeBSD. Πρόκειται για μια τεχνική λίστα. Προορίζεται για οποιονδήποτε ασχολείται ενεργά με την ανάπτυξη ή τη μεταφορά εφαρμογών Mono ή C# στο FreeBSD. Η συζήτηση αφορά την επίλυση προβλημάτων η την εύρεση εναλλακτικών λύσεων. Άτομα που ενδιαφέρονται να παρακολουθήσουν την τεχνική συζήτηση είναι επίσης ευπρόσδεκτα.

freebsd-office

Εφαρμογές γραφείου στο FreeBSD

Συζητήσεις σχετικές με την εγκατάσταση, ανάπτυξη και υποστήριξη εφαρμογών γραφείου στο FreeBSD.

freebsd-performance

Συζητήσεις για την ρύθμιση και την βελτιστοποίηση του FreeBSD

Αυτή η λίστα υπάρχει για να παρέχει ένα μέρος όπου οι hackers, οι διαχειριστές, και όσοι άλλοι ενδιαφέρονται, να συζητούν θέματα σχετικά με την απόδοση του FreeBSD. Αποδεκτά θέματα είναι οι συζητήσεις που αναφέρονται σε εγκαταστάσεις FreeBSD που υπόκεινται σε μεγάλο φόρτο, έχουν προβλήματα απόδοσης, ή φτάνουν το FreeBSD στα όρια του. Συνιστούμε ανεπιφύλακτα να γραφούν στη λίστα όσοι ενδιαφέρονται να βελτιώσουν την απόδοση του FreeBSD. Είναι μία τεχνική λίστα που απευθύνεται σε έμπειρους χρήστες του FreeBSD, hackers, ή διαχειριστές που ενδιαφέρονται να κάνουν το FreeBSD γρήγορο και αξιόπιστο. Δεν πρόκειται για μια λίστα ερωτήσεων και απαντήσεων που μπορεί να αντικαταστήσει την μελέτη της τεκμηρίωσης, αλλά ένα μέρος για συνεισφορές ή για απαντήσεις σε αναπάντητα θέματα σχετικά με την απόδοση.

freebsd-pf

Συζητήσεις και ερωτήσεις για το σύστημα packet filter firewall

Συζητήσεις σχετικές με το packet filter (pf) firewall system στο FreeBSD. Τεχνικές συζητήσεις και ερωτήσεις χρηστών είναι ευπρόσδεκτες. Η λίστα είναι επίσης ένα μέρος για συζήτηση του ALTQ QoS framework.

freebsd-platforms

Μεταφορά του FreeBSD σε μη-Intel® πλατφόρμες

Προβλήματα του FreeBSD που εμφανίζονται σε περισσότερες από μία πλατφόρμες, καθώς και γενικές συζητήσεις και προτάσεις για μεταφορά του FreeBSD σε μη-Intel® πλατφόρμες. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-ports

Συζήτηση για τα "ports"

Συζητήσεις σχετικές με την "Συλλογή των Ports" του FreeBSD (/usr/ports), την υποδομή των ports, και γενικά τις προσπάθειες συντονισμού των ports. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-ports-announce

Σημαντικές ειδήσεις και οδηγίες σχετικές με την "Συλλογή των Ports" του FreeBSD.

Σημαντικές ειδήσεις σχετικές με την "Συλλογή των Ports" (/usr/ports) που απευθυνόνται σε όσους αναπτύσσουν ή μεταφέρουν λογισμικό στο FreeBSD αλλά και στους τελικούς χρήστες. Περιλαμβάνονται ειδήσεις σχετικές με αλλαγές στην αρχιτεκτονική και την υποδομή, νέες δυνατότητες αλλά και σημαντικές πληροφορίες αναβάθμισης και νέων εκδόσεων. Πρόκειται για λίστα με μικρή κίνηση που προορίζεται για ανακοινώσεις.

freebsd-ports-bugs

Συζήτηση για τα σφάλματα των "ports"

Συζητήσεις που σχετίζονται με τις αναφορές προβλημάτων της "Συλλογής των Ports" (/usr/ports) του FreeBSD, προτάσεις για νέα ports ή για αλλαγές σε υπάρχοντα ports. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-proliant

Τεχνική συζήτηση για το FreeBSD σε διακομιστές HP ProLiant

Αυτή η λίστα είναι για τεχνικές συζητήσεις σχετικά με την χρήση του FreeBSD σε διακομιστές HP ProLiant. Η συζήτηση περιλαμβάνει θέματα προγραμμάτων οδήγησης για ProLiant, λογισμικό διαχείρισης, εργαλεία ρυθμίσεων, και ανανεώσεις του BIOS. Η λίστα αυτή είναι το καταλληλότερο μέρος για συζήτηση σχετικά με τα αρθρώματα hpasmd, hpasmcli, και hpacucli.

freebsd-python

Η Python στο FreeBSD

Αυτή η λίστα είναι για συζητήσεις σχετικές με την βελτιστοποίηση της υποστήριξης της Python στο FreeBSD. Είναι μια τεχνική λίστα. Προορίζεται για άτομα που ασχολούνται με την μεταφορά της Python, των αρθρωμάτων της (modules) και του Zope στο FreeBSD. Όσοι ενδιαφέρονται να παρακολουθήσουν την τεχνική συζήτηση, είναι ευπρόσδεκτοι.

freebsd-questions

Ερωτήσεις χρηστών

Αυτή η λίστα είναι για ερωτήσεις σχετικές με το FreeBSD. Δεν πρέπει να στέλνετε ερωτήσεις τύπου "how to" σε τεχνικές λίστες εκτός αν πιστεύετε ότι η ερώτηση σας είναι πολύ εξειδικευμένη.

freebsd-ruby

Συζήτηση σχετικά με τη Ruby στο FreeBSD

Η λίστα αυτή είναι για συζητήσεις που σχετίζονται με την υποστήριξη της Ruby στο FreeBSD. Πρόκειται για μια λίστα τεχνικών ερωτήσεων. Απευθύνεται σε άτομα που δουλεύουν σε Ports της Ruby, σε βιβλιοθήκες τρίτων κατασκευαστών, και σε άλλα πλαίσια λειτουργιών.

Είναι επίσης ευπρόσδεκτοι όσοι ενδιαφέρονται για αυτού του είδους την τεχνική συζήτηση.

freebsd-scsi

Το υποσύστημα SCSI

Αυτή η λίστα είναι για άτομα που εργάζονται στο SCSI υποσύστημα του FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

ηλεκτρονική λίστα του FreeBSD για θέματα ασφάλειας

Θέματα ασφαλείας

Αφορά θέματα ασφαλείας υπολογιστών που εκτελούν FreeBSD (DES, Kerberos, γνωστά θέματα ασφαλείας και διορθώσεις, κτλ). Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα. Σημειώστε ότι δεν πρόκειται για λίστα ερωτήσεων και απαντήσεων, αλλά η συνεισφορά (τόσο ερωτήσεων όσο ΚΑΙ απαντήσεων) στο FAQ είναι ευπρόσδεκτη.

ηλεκτρονική λίστα Ανακοινώσεων για Θέματα Ασφάλειας του FreeBSD

Ειδοποιήσεις ασφαλείας

Ειδοποιήσεις για προβλήματα ασφαλείας και διορθώσεις στο FreeBSD. Δεν πρόκειται για λίστα συζητήσεων. Η λίστα συζητήσεων είναι η FreeBSD-security.

freebsd-small

Χρήση του FreeBSD σε embedded εφαρμογές

Αυτή η λίστα συζητά θέματα σχετικά με ασυνήθιστα μικρές και embedded εγκαταστάσεις του FreeBSD. Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

Η λίστα αυτή έχει αντικατασταθεί από την freebsd-embedded.

ηλεκτρονική λίστα του FreeBSD-STABLE;

Συζητήσεις σχετικές με την χρήση του FreeBSD-STABLE

Αυτή η λίστα είναι για τους χρήστες του FreeBSD-STABLE. Περιέχει προειδοποιήσεις για νέα χαρακτηριστικά που πρόκειται να ενσωματωθούν στο -STABLE και τα οποία ενδεχομένως να επηρεάσουν τους χρήστες του. Επίσης περιέχει οδηγίες για τα βήματα που πρέπει να ακολουθήσετε ώστε να παραμείνετε στο -STABLE. Θα πρέπει να εγγραφείτε σε αυτή τη λίστα, αν ακολουθείτε το "STABLE". Είναι μια τεχνική λίστα και συζητούνται μόνο αυστηρά τεχνικά θέματα.

freebsd-standards

Συμμόρφωση με τα πρότυπα C99 POSIX

Αυτή η λίστα είναι για τεχνικές συζητήσεις σχετικά με την συμμόρφωση του FreeBSD με τα πρότυπα C99 και POSIX.

freebsd-toolchain

Συντήρηση των ενσωματωμένων εργαλείων του FreeBSD

Αυτή η λίστα είναι για συζητήσεις που σχετίζονται με την σειρά εργαλείων (toolchain) που έρχονται με το FreeBSD. Η συζήτηση μπορεί να περιλαμβάνει θέματα σχετικά με την κατάσταση του Clang και του GCC, αλλά και θέματα σχετικά με προγράμματα όπως μεταγλωττιστές, assemblers, linkers και debuggers.

freebsd-usb

Συζήτηση για την υποστήριξη του διαύλου USB στο FreeBSD

Αυτή η λίστα είναι για τεχνικές συζητήσεις σχετικά με την υποστήριξη του διαύλου USB στο FreeBSD.

freebsd-user-groups

Οργάνωση των συλλόγων χρηστών

Αυτή η λίστα είναι για τους συντονιστές των επιμέρους τοπικών συλλόγων χρηστών για συζήτηση θεμάτων μεταξύ τους και με κάποιο μέλος της ομάδας Core. Αυτή η λίστα θα πρέπει να αναφέρει μόνο τις συναντήσεις και την οργάνωση projects που αναφέρονται σε περισσότερους από ένα συλλόγους χρηστών.

freebsd-vendors

Πωλητές

Οργάνωση συζητήσεων μεταξύ του FreeBSD Project και των πωλητών λογισμικού και υλικού σχετικού με το FreeBSD.

freebsd-virtualization

Συζήτηση διάφορων τεχνικών εικονικοποίησης που υποστηρίζονται από το FreeBSD.

Μια λίστα για τη συζήτηση των διάφορων τεχνικών εικονικοποίησης που υποστηρίζονται από το FreeBSD. Από τη μια μεριά εστιάζει στην υλοποίηση των βασικών λειτουργιών αλλά και την προσθήκη νέων δυνατοτήτων. Από την άλλη, οι χρήστες θα έχουν μια ομάδα συζητήσεων όπου μπορούν να ζητούν βοήθεια σε περίπτωση προβλημάτων, ή να συζητούν τις δικές τους χρήσεις.

freebsd-wip-status

Κατάσταση εργασιών σε εξέλιξη στο FreeBSD

Στη λίστα αυτή μπορείτε να ανακοινώσετε την έναρξη και την πρόοδο κάποιας εργασίας σας που σχετίζεται με το FreeBSD. Τα μηνύματα σε αυτή τη λίστα ελέγχονται. Συνίσταται να στείλετε το μήνυμα σας με παραλήπτη μια πιο τοπική σας λίστα του FreeBSD, και απλώς να κοινοποιήσετε το μήνυμα σας σε αυτή τη λίστα. Με τον τρόπο αυτό, μπορείτε επίσης να συζητήσετε για την εργασία σας στην τοπική λίστα, καθώς η συζήτηση σε αυτή τη λίστα δεν επιτρέπεται.

Δείτε τα αρχεία της λίστας για να πάρετε μια ιδέα της μορφής των μηνυμάτων που μπορείτε να στείλετε.

Μια περίληψη των περιεχομένων της λίστας ενδέχεται να δημοσιεύεται κατά τακτά διαστήματα στη δικτυακή τοποθεσία του FreeBSD, ως μέρος των Αναφορών Κατάστασης (Status Reports) .

Στην ίδια τοποθεσία, μπορείτε επίσης να βρείτε περισσότερα παραδείγματα και προηγούμενες αναφορές.

freebsd-wireless

Συζήτηση σχετικά με τη στοίβα 802.11, τα εργαλεία ασύρματου δικτύου και την ανάπτυξη προγραμμάτων οδήγησης

Η λίστα αυτή εστιάζει στη στοίβα δικτύου 802.11 (sys/net80211), την ανάπτυξη προγραμμάτων οδήγησης και εργαλείων. Περιλαμβάνει αναφορές προβλημάτων, νέα χαρακτηριστικά και πληροφορίες συντήρησης.

freebsd-xen

Συζήτηση για τη μεταφορά του FreeBSD στο Xen™ - υλοποίηση και χρήση

Πρόκειται για μια λίστα που εστιάζει στην μεταφορά του FreeBSD στο Xen™. Η κίνηση σε αυτή τη λίστα αναμένεται να είναι μικρή, και έτσι θα χρησιμοποιηθεί τόσο για τεχνικές συζητήσεις σχετικά με το σχεδιασμό και την υλοποίηση, όσο και με προβλήματα εγκατάστασης και διαχείρισης.

freebsd-xfce

XFCE

Συζήτηση για τη μεταφορά του XFCE στο FreeBSD. Πρόκειται για μια λίστα τεχνικών συζητήσεων. Προορίζεται για όσους ασχολούνται ενεργά με τη μεταφορά του XFCE στο FreeBSD ώστε να συζητούν προβλήματα και εναλλακτικές λύσεις. Η λίστα είναι επίσης ανοικτή σε όσους ενδιαφέρονται για τεχνική συζήτηση αυτού του είδους.

freebsd-zope

Zope

Μια λίστα συζητήσεων σχετικών με τη μεταφορά του περιβάλλοντος Zope στο FreeBSD. Πρόκειται για λίστα τεχνικών συζητήσεων. Απευθύνεται κυρίως σε άτομα που συμμετέχουν ενεργά στη μεταφορά του Zope στο FreeBSD και συζητούνται προβλήματα και εναλλακτικές λύσεις. Η λίστα είναι επίσης ανοικτή σε όσους ενδιαφέρονται για τεχνική συζήτηση αυτού του είδους.

C.1.4. Φιλτράρισμα στις Λίστες Ηλεκτρονικού Ταχυδρομείου

Οι λίστες ηλεκτρονικού ταχυδρομείου του FreeBSD φιλτράρονται με πολλαπλούς τρόπους για να αποφύγουμε την διανομή spam, ιών, και άλλων ανεπιθύμητων μηνυμάτων. Το φιλτράρισμα που περιγράφεται σε αυτή την ενότητα, αποτελεί ένα μόνο μέρος των συνολικών μέτρων που λαμβάνουμε για την προστασία των λιστών ηλεκτρονικού ταχυδρομείου.

Στις λίστες επιτρέπονται μόνο συγκεκριμένοι τύποι συνημμένων αρχείων. Όλα τα συνημμένα αρχεία με τύπο MIME που δεν βρίσκεται στην παρακάτω λίστα, διαγράφονται πριν διανεμηθεί το μήνυμα στις λίστες.

- application/octet-stream
- application/pdf

- application/pgp-signature
- application/x-pkcs7-signature
- message/rfc822
- multipart/alternative
- multipart/related
- multipart/signed
- text/html
- text/plain
- text/x-diff
- text/x-patch

Μερικές λίστες μπορεί να επιτρέπουν συνημμένα αρχεία και άλλων τύπων MIME, αλλά οι παραπάνω τύποι ισχύουν στις περισσότερες λίστες.

Εάν το κείμενο ενός μηνύματος περιέχεται τόσο σε μορφή HTML όσο και απλού κειμένου, το τμήμα HTML θα αφαιρεθεί. Εάν ένα μήνυμα περιέχει μόνο HTML, θα μετατραπεί σε απλό κείμενο.

C.2. Usenet Newsgroups

Εκτός από δύο newsgroups που ασχολούνται με το FreeBSD, υπάρχουν πολλά ακόμα στα οποία γίνεται συζήτηση για το FreeBSD ή άλλα θέματα που ενδεχομένως ενδιαφέρουν τους χρήστες του.

C.2.1. Newsgroups Σχετικά με το BSD

- comp.unix.bsd.freebsd.announce
- comp.unix.bsd.freebsd.misc
- de.comp.os.unix.bsd (Στα Γερμανικά)
- fr.comp.os.bsd (Στα Γαλλικά)
- it.comp.os.freebsd (Στα Ιταλικά)
- tw.bbs.comp.386bsd (Σε Παραδοσιακά Κινέζικα)

C.2.2. Άλλα Ενδιαφέροντα UNIX® Newsgroups

- comp.unix
- comp.unix.questions
- comp.unix.admin
- comp.unix.programmer
- comp.unix.shell
- comp.unix.user-friendly
- comp.security.unix

- comp.sources.unix
- comp.unix.advocacy
- comp.unix.misc
- comp.bugs.4bsd
- comp.bugs.4bsd.ucb-fixes
- comp.unix.bsd

C.2.3. Σύστημα X Window

- comp.windows.x.i386unix
- comp.windows.x
- comp.windows.x.apps
- comp.windows.x.announce
- comp.windows.x.intrinsics
- comp.windows.x.motif
- comp.windows.x.pex
- comp.emulators.ms-windows.wine

C.3. Διακομιστές Ιστοσελίδων

Central Servers, Armenia, Australia, {mirrors-austria}, Czech Republic, Denmark, Finland, France, Germany, Hong Kong, Ireland, Japan, Latvia, Lithuania, Netherlands, Norway, Russia, Slovenia, South Africa, Spain, Sweden, Switzerland, Taiwan, United Kingdom, United States of America.

(as of UTC)

Central Servers

- https://www.FreeBSD.org/

Armenia

- http://www1.am.FreeBSD.org/ (IPv6)

Australia

- http://www.au.FreeBSD.org/
- http://www2.au.FreeBSD.org/

{mirrors-austria}

- http://www1.am.FreeBSD.org/ (IPv6)

Czech Republic

- http://www.cz.FreeBSD.org/ (IPv6)

Denmark

- http://www.dk.FreeBSD.org/ (IPv6)

Finland

- http://www.fi.FreeBSD.org/

France

- http://www1.fr.FreeBSD.org/

Germany

- http://www.de.FreeBSD.org/

Hong Kong

- http://www.hk.FreeBSD.org/

Ireland

- http://www.ie.FreeBSD.org/

Japan

- http://www.jp.FreeBSD.org/www.FreeBSD.org/ (IPv6)

Latvia

- http://www.lv.FreeBSD.org/

Lithuania

- http://www.lt.FreeBSD.org/

Netherlands

- http://www.nl.FreeBSD.org/

Norway

- http://www.no.FreeBSD.org/

Russia

- http://www.ru.FreeBSD.org/ (IPv6)

Slovenia

- http://www.si.FreeBSD.org/

South Africa

- http://www.za.FreeBSD.org/

Spain

- http://www.es.FreeBSD.org/
- http://www2.es.FreeBSD.org/

Sweden

- http://www.se.FreeBSD.org/

Switzerland

- http://www.ch.FreeBSD.org/ (IPv6)
- http://www2.ch.FreeBSD.org/ (IPv6)

Taiwan

- http://www.tw.FreeBSD.org/
- http://www2.tw.FreeBSD.org/
- http://www4.tw.FreeBSD.org/
- http://www5.tw.FreeBSD.org/ (IPv6)

United Kingdom

- http://www1.uk.FreeBSD.org
- http://www3.uk.FreeBSD.org/

United States of America

- http://www5.us.FreeBSD.org/ (IPv6)

C.3.1. Forums, Blogs, και Κοινωνικά Δίκτυα

- Τα Forums του FreeBSD βασίζονται σε διεπαφή web και είναι κατάλληλα για τεχνικές συζητήσεις και ερωτήσεις που αφορούν το FreeBSD.
- Το Planet FreeBSD συγκεντρώνει σε ένα σημείο τις ροές από δεκάδες ιστολόγια μελών της ομάδας ανάπτυξης του FreeBSD. Πολλά από τα μέλη, χρησιμοποιούν αυτή τη δυνατότητα για να γνωστοποιήσουν την εργασία που κάνουν τη δεδομένη στιγμή, τυχόν νέες διορθώσεις, καθώς και τα μελλοντικά τους σχέδια.
- Το κανάλι BSDConferences στο Youtube παρέχει μια συλλογή βίντεο υψηλής ποιότητας, από διάφορα BSD συνέδρια σε όλο τον κόσμο. Πρόκειται για ένα θαυμάσιο τρόπο να παρακολουθήσετε σημαντικά μέλη της ομάδας ανάπτυξης να παρουσιάζουν τη νέα τους δουλειά στο FreeBSD.

C.3.2. Επίσημα Mirrors

C.4. Διευθύνσεις Ηλεκτρονικού Ταχυδρομείου

Οι ακόλουθες ενώσεις χρηστών παρέχουν στα μέλη τους διευθύνσεις ηλεκτρονικού ταχυδρομείου που σχετίζονται με το FreeBSD. Ο διαχειριστής που αναφέρεται παρακάτω, διατηρεί το δικαίωμα να ανακαλέσει την διεύθυνση, αν γίνει κατάχρηση της με οποιοδήποτε τρόπο.

Τομέας	Υπηρεσίες	Ένωση Χρηστών	Διαχειριστής
ukug.uk.FreeBSD.org	Μόνο προώθηση	ukfreebsd@uk.FreeBSD.org	Lee Johnston lee@uk.FreeBSD.org

Appendix D: Κλειδιά PGP

Στο παράρτημα αυτό, θα βρείτε τα δημόσια PGP κλειδιά των officers και των μελών της ομάδας ανάπτυξης του FreeBSD. Μπορείτε να τα χρησιμοποιήσετε για να ελέγξετε μια ψηφιακή υπογραφή ή για να στείλετε κρυπτογραφημένο email σε κάποιο μέλος της ομάδας. Μπορείτε να κατεβάσετε την πλήρη λίστα από κλειδιά χρηστών του FreeBSD.org, από την τοποθεσία pgpkeyring.txt.

D.1. Officers

D.1.1. Ομάδα Ασφάλειας <security-officer@FreeBSD.org>

```
pub   rsa4096/D9AD2A18057474CB 2022-12-11 [C] [expires: 2030-01-24]
      Key fingerprint = 0BE3 3275 D74C 953C 79F8  1107 D9AD 2A18 0574 74CB
uid                           FreeBSD Security Officer <security-officer@freebsd.org>
sub   rsa4096/6E58DE901F001AEF 2022-12-11 [S] [expires: 2028-01-24]
sub   rsa4096/46DB26D62F6039B7 2022-12-11 [E] [expires: 2028-01-24]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGOVdeUBEADHF5VGg1iPbACB+7lomX6aDytUf0k2k2Yc/Kp6lfYv7JKU+1nr
TcNF7Gt1YkajPSeWRKNZw/X94g4w5TEOHbJ6QQWx9g+N7RjEq75actQ/r2N5zY4S
ujfFTepbvgR55mLTxlxGKFBmNrfNbpHRyh4GwFRgPlxf5Jy9SB+0m54yFS4QlSd0
pIzO0CLkjHUFy/8S93oSK2zUkgok5gLWruBXom+8VC3OtBElkWswPkE1pKZvMQCv
VyM+7BS+MCFXSdZczDZZoEzpQJGhUYFsdg0KqlLv6z1rP+HsgUYKTkRpcrumDQV0
MMuCE4ECU6nFDDTnbR8Wn3LF5oTt0GtwS0nWf+nZ1SFTDURcSPR4Lp/PKjuDAkOS
P8BaruCNx1ItHSwcnXw0gS4+h8FjtWNZpsawtzjjgApcl+m9KP6dkBcbN+i1DHm6
NG6YQVtVWyN8aOKmoC/FEm1CWh1bv+ri9XOkF2EqT/ktbjbT1hFoFGBkS9/35y1G
3KKyWtwKcyF4OXcArl6sQwGgiYnZEG3sUMaGrwQovRtMf7le3cAYsMkXyiAnEufa
deuabYLD8qp9L/eNo+9aZmhJqQg4EQb+ePH7bGPNDZ+M5oGUwReX857FoWaPhs4L
dAKQ1YwASxdKKh8wnaamjIeZSGP5TCjurH7pADAIaB3/D+ZNl2a7od+C1wARAQAB
tDdGcmVlQlNEIFNlY3VyaXR5IE9mZmljZXIgPHNlY3VyaXR5LW9mZmljZXJAZnJl
ZWJzZC5vcmc+iQJSBBMBCgA8AhsBBAsJCAcEFQoJCAUWAgMBAAIeBQIXgBYhBAvj
MnXXTJU8efgRB9mtKhgFdHTLBQJjlXeQBQkF3u+rAAoJENmtKhgFdHTLOVoQALS3
cj7rqYkHiV4zDYrgPEp9O1kAyGI8VdfGAMkDVTqr+wP4v/o7LIUrgwZl5qxesVFB
VknFr0Wp5g9h0iAjasoI5sDd6tH2SmumhBHXFVdftzDQhrugxH6fWRhHs0SaFYCk
Qt5nFbcpUfWgtQ35XTbsL8iENdYpjKXsSFQrJneGSwxIjWYTFn6ps/AI3gwR8+Bn
OffEFdYugJ049O6Vu6YBFJHrnMO7NbF4v95dVYuLtpMIaXWM+V9KITmhaBzFz5fM
Q7UOzcLlbxOYKNIWcp8QQk429mayKW5VUeUExUD1ZzBHn+P6ZG7QTMDu/RmBqiHo
ewCMVz4n9uXT5BiOngE4CvS0WQwHzK+k9MLpG2u/Bo9+LT0Ceh9Ou1rfU5+0tRwl
GyOFFjf3INS7I7gkcAwxQ7dzDItN/UQPZpg8y9mABU2x4enz0AvTnb61d/1dnTEr
tdNgU433he0ZnD1HurZCjBEWC656wv6iMdWcD8gjhMbmEpPmjvXcYlTO6zhEygSM
DiwdQCWK2W4++YJerA6ULBi3niNWBpofOFH8XylV56ruhjtHCo7+/3carcMoPOJv
lVZ1zCKxLro3TRBT15JTFBGqblRyTopFK3PuxW//GTnZOtpQEOV6yL4RAXcWeC1d
1hb5k/YxUmRF6XsDNEH4b08T8ZO8dV3dAV43Wh1oiQEzBBABCAAdFiEEuyjUCzYO
7pNq7RVv5fe8y6O93fgFAmObXVYACgkQ5fe8y6O93fiBlwf/W8y1XXJIx1ZA3n6u
f7aS70rbP9KFPr4U0dixwKE/gbtIQ9ckeNXrDDWz0v0NCz4qS+33IPiJg1WcY3vR
W90e7QgAueCo5TdZPImPbCs42vadpa5byMXS4Pw+xyT+d/yp2oLKYbj3En4bg1GM
```

```
w71DezIjvV+e01UR++u1t9yZ8LOWM5Kumz1zyQLZDZ8qIKt1bBfpa+E0cEqtNQWu
iGhQE3AHI8eWV+jBkg5y2zHRIevbWb1UPsj43lgkFtAGHk9rrM8Rmgr4AXr531iD
srBwauKZ/MElcF3MINuLH+gkPPaFHw/YIpLRLaZXZVsw3Xi1RNXI2n2ea29dvs/C
Lcf1vYkCMwQQAQgAHRYhBPwOh4rlr+eIAo1jVdOXkvSep+XCBQJjm14FAAoJENOX
kvSep+XC0DcP/1ZB7k9p1T+9QbbZZE1PJiHby3815ccH3XKexbNmmakHIn3L6Cet
F891Kqt9ssbhFRMNtyZ/k/8y8Hv5bKxVep5/HMyK+8aqfDFN0WMrqZh0/CiR6DJh
gnAmPNw/hAVHMHaYGII9kCrFfPFJ02FKoc81g9F08odb7TV+UlvRjkErhRxF+dGS
wQoO0RCbf0Z1cs7nd0Vb2z4IJh4XMxBjWc/uQ2Q9dH/0uRzwpAnR4YX+MG5YrX7Z
zBvDyR0r76iQwRSDKgioNgkr6R3rq1NZGdaj+8b0LzdOqtzKJ/eupDe3+H67e/EN
qymtreGjrubpiU9bKvYArisUqhE5KtguryvR6Qz9bj87nPg33DT3WWGVrwFRxBox
dbWzjQFv0wug8m4GAwVF7fPR5/eW7IHw8zvgn0vSPcZz7MZ4e6Y5jN4kA5/xWJYZ
Sps54qQWB+FA30unIXN68KqdIzONIbtaY3W4/JjJUCm4T+wEjKaH+wJX8w1DMjlg
mkTmGh/UrTyC1vXbPgk9Sy3cRTICR1T9z7W8UlmTtnKrUklrjlFR7SXzrEXzLGOX
Fm+NEHpHNXqzcm6c3QfzY/yQ9HSAQ/t7SUQ9caRePbDz3/msyPxtGFor9roQv6VN
wRXCyRgkH4Y5tPhJAQ8G/FxX+VXFb93QL0lfelb23/BBu6cUwW63SRn5iHUEExYI
AB0WIQQeB2Johg/5/ikUnJwDU9SVF1S13AUCZISO3wAKCRADU9SVF1S13NnqAP95
LA1Om9XSAKl76VtV+L3JPDdAwIdbNa0OsRT4Wm7U3wD/YoFrdHXVHHQFKwYeUUhj
XZcxnZLe9Ixo0/JP+RVFVw6JAlIEEwEKADwCGwEECwkIBwQVCgkIBRYCAwEAAh4F
AheAFiEEC+MydddMlTx5+BEH2a0qGAV0dMsFAmluhFoFCQ1lXf0ACgkQ2a0qGAV0
dMv8ixAAhYn3uxnjTCBZ5BJ6FMdwFXgGZMZVnL1qEoHA7HWB0ZoQlu29sFzBX97x
rkVZfWiU82V9/PYyHh4EY0hN9oOJMDDhSgi+DfdoEablIcIXR9uBBL/Snnak6uEF
gOD6VFH1T3o7iBmS/ixee2YFXq5QxAwEiANSAsxDm2rlyztPc5xM76fz5eEcgp1m
UDI7qFjoEkJVvRraJGVy3AUh4sr/94VAXPuCa7JnC6a8j9SD8XtzqIfcuqNBXXfA
m4ji4fN+KcDHtZPdkNLDBu1DEXQkOR/1S++NmXHYCEdQEuVOwLVsy6vQqgc+unju
Xh9sOrdiXUWylHh2hvgmwkjhMGOREiIRwNoA09m0OKZ2jo2dSlhNdVFRD5yhD92t
X9BarQbbjQtyCvoWnCJMFfw/vDnxfDdUdV3GxLhaOWvR8ItWQ7ts8tEZSjR/G76/
fHj1JRNuHRdhwype6ehieewJSMyzByhT0A3Njv3KLI4nwQj//MYzB5FJ9uOmKLcG
w7PB0yVjW4oRbG62+Qv6IQybCyrAL+12qgbUXbMsTqMwmsmdgtsqr/7OJNo3PBxX
2rUEio/mez8wuzNB0mJtlMynoMqXtbFX7AAXHk16fOGd6L6guW8+IhPedT3TvrjS
hqiQVvjOhM6rEYZ/YUfcIdkWJVpmE6+MRPVUufyMWeHaWqsKXoa5Ag0EY5V2yQEQ
AOqjzPpMUCGu8eElXnAd2PruC6hi+lc/yC90KqizxIuW6qLQBaAkTCWq7suYpDqo
ygn7YM3rL50S285WAECAXrcst/cVAqr0UH/e6p4iJCUIiXcfjd/wq20RnN/+VuvL
hjpCFLY5czfVS31D7Uh9MbC+zUTz8nVTiNCsAao0qSdfJDIzB4nSO+9xIsme/dLs
I5QlU5PdxOBV6HdEhCUXOoratJCbKAOlLxtPwyMKxmv4oZ7Mqlt10peKjhpBb97q
cIzJhHxujQZD0OmzIA6xoQ2eSCGdxCEDsZ09kr3Esw1AwKnQ51xmWpFWNFk6627M
1bo8+hzOz81CrTZhYrgE+1JXv6V1L2A9lMsimdE1BHNycDS+dBOpIB9qxXCwAab4
ykfvNxox/ZPDUrTy7v7mDI5uDNTNCYYsKCj1UidycOKzSziB9Oa2uvmMJ5XstgNB
f7Z8Cky1dtVd4ol6bU9L5nos9tbYeSXFi4bmcWB7AJiVCMq6N+LBbUKWGLglB4TU
1qhttpqv31X9V6ges5gARY/RuRTKsVyhwsn7SDcqmNKRy0im2AYakwEp7hT07ula
hOSLxjP+5hCf+nSJlwbxJ8ozwjjbzeN2yLlJSI00klkIFBNUDt3wzFRW/n6qlf+/
lepgzekfNrYMtfPB8AT07Z2A3U4xlgiV346dZymbY/EjABEBAAGJBHIEGAEKACYW
IQQL4zJ110yVPHn4EQfZrSoYBXR0ywUCY5V2yQIbAgUJAgIpAAJACRDZrSoYBXR0
y8F0IAQZAQoAHRYhBLYVJ36BCH33XIGDO25Y3pAfABrvBQJjlXbJAAoJEG5Y3pAf
ABrvuBsQAOlQFPXhx6whO4yw5ZizIS02YHhSVMVYKS2T9jPIKi1qxnEiEw9eKH0b
W0Oj0TEhZPyM2NJID7DRWK5r8+KsMu8jwm1fUmIrefAx6fCVfCWRECT1MlbL3jhh
6AcX/nK2e3Bn8vgExhzczO3JlvD6wPCc0FkpiY7yDB9ihu1+gbE5Hg6dvftttRXD
rbEdAifbNp9KYxDigxdlOb0S14hjCBysLWH5Su/khcIlkeuqZcI8TmDldnUb2OqT
CVpFhaNwsPSrHBzmb0s2sXo4FL03pLsOdwhi31W6kjk4KvW5FKrOpoEwUMKVNMf5
0DHdvonUoUHRSIc/cV5NqUWHwvc0T5031qk0CCRRa/+/iij/p2RG7c1mx7ZECj+j
ZfmvjSqT+WHJ1BFlNJMWyK4fdVRZWyCaoAecdbukwzDwUCUqHJFIWeFtbut7SOPx
cwg7sbnKNApAKdi491dvH75s/U/OwRYO/2P+ymHlqtyix2jq0ReSVYcQPXswQ8i2
```

```
ifX41F+xTSl4RWCBBeXB1Nxk3+HsV4Jnnp1zAJZ0KlKW/oJxbNFdI1TImkpr2p8i
oFf+aiePLvDkgeaG8vABgjoihPXWHVAMR8Z+GvBY/A6OdexpibkTvC/zDr0/Exs4
lsylZKDwvvFbctcpHVXBeCBQLX5vfLrsTkaCLWF/SV9OdMykvYKU7ZAP+gKEwhp+
HPFuOHZbOBhqFUdkfeCkdzX/QGdzTuz349roRhgz2vRfN7MtbtuzA6NWWhEWt5Dc
UgX/Y5I3Q4Z2bt3JiXQ6WJMgMMOXAr+XxtxyRRykc1HV3DQ/cq8OWYubNnIbgebP
NIFr2OIWKsR9yDaucZzpmLfzaMZUAu5hWmU9fIw5SIKGnQABBnNMhilfD+CkETp6
baTvjTK4rpaobjJdeCTrsWgfXRNC8x3hDvcrjPD70MylOGVQdx8GYChWJnCKXsLT
GX7KwdfxkjclTyzWvdcCemp0eLhamLGb9y1dtWdNIDcVCvZJy0lipHVUdFYYxb4i
LZJANL631tlPM6AA8sO1/L4mqEGnAIHVrUQd+2QkSiOl9mKlpgaR/fJz683BR5Qe
n9ywX0JPtBupqPW3t9VbO/uNxUqlHCeAhPi9NLOpujpYLfgW5QAfS3u0nkp5nrbk
CoQUua2q0Oj7J0mFmtWtcE1c9+THmFJVb8j2G9yQw3ADe3Qp9ALazP5nVDVri8NZ
BhHK1/KuBmRYZtcyfqXUnKoiiWAlm5rHaRiztW7e3wqm2oJu/RkEAagybutEuBWh
2Ej2+gDxjEKKtIKGu54lif4kqTwwjKTcN1ekGihwwgCMUkBSBeNXk1ClkzLFHwES
JCcFwdEgpVYQTKFsu0emYISyco3IpUajGzfUiQRyBBgBCgAmAhsCFiEEC+MydddM
lTx5+BEH2a0qGAV0dMsFAmWFy28FCQPyfaYCQMF0IAQZAQoAHRYhBLYVJ36BCH33
XIGDO25Y3pAfABrvBQJjlXbJAAoJEG5Y3pAfABrvuBsQAOlQFPXhx6whO4yw5Ziz
IS02YHhSVMVYKS2T9jPIKi1qxnEiEw9eKH0bW0Oj0TEhZPyM2NJID7DRWK5r8+Ks
Mu8jwm1fUmIrefAx6fCVfCWRECT1MlbL3jhh6AcX/nK2e3Bn8vgExhzczO3JlvD6
wPCc0FkpiY7yDB9ihu1+gbE5Hg6dvftttRXDrbEdAifbNp9KYxDigxdlOb0S14hj
CBysLWH5Su/khcIlkeuqZcI8TmDldnUb2OqTCVpFhaNwsPSrHBzmb0s2sXo4FL03
pLsOdwhi31W6kjk4KvW5FKrOpoEwUMKVNMf50DHdvonUoUHRSIc/cV5NqUWHwvc0
T5031qk0CCRRa/+/iij/p2RG7c1mx7ZECj+jZfmvjSqT+WHJ1BFlNJMWyK4fdVRZ
WyCaoAecdbukwzDwUCUqHJFIWeFtbut7SOPxcwg7sbnKNApAKdi491dvH75s/U/O
wRYO/2P+ymHlqtyix2jq0ReSVYcQPXswQ8i2ifX41F+xTSl4RWCBBeXB1Nxk3+Hs
V4Jnnp1zAJZ0KlKW/oJxbNFdI1TImkpr2p8ioFf+aiePLvDkgeaG8vABgjoihPXW
HVAMR8Z+GvBY/A6OdexpibkTvC/zDr0/Exs4lsylZKDwvvFbctcpHVXBeCBQLX5v
fLrsTkaCLWF/SV9OdMykvYKUCRDZrSoYBXR0yyOqEACitDvbkbfjaton6izr4T8Q
U2yvhJHkf4B6KeVDbKY1J4784OxXp2bJgPeF53SYBe8gm3YHjp8ULh4A/19U4hsw
yE8ymcm5nIs8OLyBdxkuBZJGEnzxH3woiyYqWH7991kzhEjUkuMgKLuTI1HiO0oL
MuPQNhUHOnWafSVPC0XO/tIL12OmoUuc7ligY9Z9AceFjTZOuHamixHAAc6hpxdI
W+yhC/qTpc2VK0niWeuQfq3453iRTf9MnR5Beztl3ZYRWcx7UiFuKGwZwBibNnNm
Us6GyQcJ5UTa1oeJcLqHi0Lf/r0jXo3wgJq7EZjjVyU+GI2ZVoDOaS6c4/OvLm62
XoeSlnn/dQxUcjUki+x8lb69IxSF1xAgsC/oNtFZYd5rHdlnqIBUYK0lLtSCXBkz
VeivSiQa0hL5on8LDu1nw2bXyW61yt/YxVb4FanMxAqdYVBhOfU0RaPNifH01rbb
4TwC9bTZN1LQ1KI/Swb/SruUE0RyT28fhYRtsReS2PnUODghJSFDJbwFbBZf6RKI
16q1xqKRRvxIWPm+lMOi1NLOKR9P+OKy9HmChMw0UJUcVl1cJ2xtRl3wi5t6AA6H
oNv/TrLeYVgMR9wYmKlpvjTQ5jTdrbHD1XP5jGsp8QsJMGja1m/7cryReCpcVxvI
meReaOdgz+zDmQqq3O5zuIkEcgQYAQoAJgIbAhYhBAvjMnXXTJU8efgRB9mtKhgF
dHTLBQJnhEEJBQkF0/JAAkDBdCAEGQEKAB0WIQS2FSd+gQh991yBgztuWN6QHwAa
7wUCY5V2yQAKCRBuWN6QHwAa77gbEADpUBT14cesITuMsOWYsyEtNmB4UlTFWCkt
k/YzyCotasZxIhMPXih9G1tDo9ExIWT8jNjSSA+w0Viua/PirDLvI8JtX1JiK3nw
MenwlXwlkRAk9TJWy944YegHF/5ytntwZ/L4BMYc3MztyZbw+sDwnNBZKYmO8gwf
YobtfoGxOR4Onb37bbUVw62xHQIn2zafSmMQ4oMXZTm9EteIYwgcrC1h+Urv5IXC
JZHrqmXCPE5g5XZ1G9jqkwlaRYWjcLD0qxwc5m9LNrF6OBS9N6S7DncIYt9VupI5
OCr1uRSqzqaBMFDClTTH+dAx3b6J1KFB0UiHP3FeTalFh8L3NE+dN9apNAgkUWv/
v4oo/6dkRu3NZse2RAo/o2X5r40qk/lhydQRZTSTFsiuH3VUWVsgmqAHnHW7pMMw
8FAlKhyRSFnhbW7re0jj8XMIO7G5yjQKQCnYuPdXbx++bP1PzsEWDv9j/sph5arc
osdo6tEXklWHED17MEPIton1+NRfsU0peEVggQXlwdTcZN/h7FeCZ56dcwCWdCpS
lv6CcWzRXSNUyJpKa9qfIqBX/monjy7w5IHmhvLwAYI6IoT11h1QDEfGfhrwWPwO
jnXsaYm5E7wv8w69PxMbOJbMpWSg8L7xW3LXKR1VwXggUC1+b3y67E5Ggi1hf0lf
TnTMpL2ClAkQ2a0qGAV0dMsNxRAAsuW1aLh+hgydW+iH6DmdQRMESsB1kE02kO14
```

```
62TAQaziIAvNoxw5h48xvyEnrDA8d+9IDMyxdrLmAbndUlSveMa9+EPiGHwr6VTy
FL8nA5F7DcFi4mjEyGKe18JcaAlYUtvHgWH6EjiX2iSXpsrJFEhtfFNolZ5sp9LF
I6hOBihSJxZK4sbMR7Q6IkDuAVpTFLiejBRlsXpFvTGL6040CtxbL5cqkVMYP38r
FMTuc3pGGJA4wb5EC1dGjUi6XjbYH7kuCAFyXqV9eQQP61x7K9W8qnXW+weCIMKf
SX7AcCtH1jXBAM6lqpPrh6amc+/rbg2eNA7DmgJnEY4apIcDB/b4khRMga2ozeGW
WyIvOaVvR2R7ALQ+Rgut85cM+4+Vl2PHmOzW/yYdHVb5REQItFR5COb/mGUqYhkC
tiV3nXo/K0uOQKu5SBbNzLuNvuwdn+Eimxjl18VnrGG7sjtUa0MLmtr62GiEVrhr
Dqa/biHp8LdWkAQjLZ4aTRh2XZiggaVFZHmkw3ILPyKKM21UXdM0YRk3TGVK8ODQ
y58ebPS4v9yYT9gUA9UDkDYeGcF2qjoDPVNvcG6H8jCSsPRl1KZwtqqITCOSAIAP
I4Nu97kO6nbOyQpYlwjd1MhvVXnP66mHSvmqaxbNGX1mF9B/yERkBkooNZrKuJSv
BTC2J1qJBHIEGAEKACYCGwIWIQQL4zJ110yVPHn4EQfZrSoYBXR0ywUCaW6EcgUJ
CaGkeQJAwXQgBBkBCgAdFiEEthUnfoEIffdcgYM7bljekB8AGu8FAmOVdskACgkQ
bljekB8AGu+4GxAA6VAU9eHHrCE7jLDlmLMhLTZgeFJUxVgpLZP2M8gqLWrGcSIT
D14ofRtbQ6PRMSFk/IzY0kgPsNFYrmvz4qwy7yPCbV9SYit58DHp8JV8JZEQJPUy
VsveOGHoBxf+crZ7cGfy+ATGHNzM7cmW8PrA8JzQWSmJjvIMH2KG7X6BsTkeDp29
+221FcOtsR0CJ9s2n0pjEOKDF2U5vRLXiGMIHKwtYflK7+SFwiWR66plwjxOYOV2
dRvY6pMJWkWFo3Cw9KscHOZvSzaxejgUvTekuw53CGLfVbqSOTgq9bkUqs6mgTBQ
wpU0x/nQMd2+idShQdFIhz9xXk2pRYfC9zRPnTfWqTQIJFFr/7+KKP+nZEbtzWbH
tkQKP6Nl+a+NKpP5YcnUEWU0kxbIrh91VFlbIJqgB5x1u6TDMPBQJSockUhZ4W1u
63tI4/FzCDuxuco0CkAp2Lj3V28fvmz9T87BFg7/Y/7KYeWq3KLHaOrRF5JVhxA9
ezBDyLaJ9fjUX7FNKXhFYIEF5cHU3GTf4exXgmeenXMAlnQqUpb+gnFs0V0jVMia
SmvanyKgV/5qJ48u8OSB5oby8AGCOiKE9dYdUAxHxn4a8Fj8Do517GmJuRO8L/MO
vT8TGziWzKVkoPC+8Vty1ykdVcF4IFAtfm98uuxORoItYX9JX050zKS9gpQJENmt
KhgFdHTLozcQAJCdYMPo1SPgxxRI40BCD4ekuA6ZMzdTuuso9XTTLf3moh+eu0Y+
Pv6ISOFI93g09V34H3XnuaOnA16DyApO6mCPZ58DunjRRYHv4wxbeff6vw9twPQb
bcdNgI2ZXSKjUef4FygkpUhy6075m6zoUfcsR/22Ggzd8Qw3chfoqiBZs7SlGwEH
sxkB+dJvgCMwYaLGqS9lNbHSEFnETb0ihFSHKDrK6pYrFnfsuArJN5owuTN+dzim
8g0agB3Pzs4A6+9Hpt9sN78VEY+ZzFhQD8knEgqSNbFIaNxsG5/L8/RcXuNyPvvz
5MIkhfacOX37YFfAhCORfN3PaVWYQ7oDnv8Nh69i9SkxXKUcwX0/iYaim8pwwM6a
HXhTlqBgKR5b5Hcx6Cwx1GTRUpdbJYThmz7LQgzjBIhmoGbxR3vyJjSyPGBZa3Ih
jAETYzMt7j0qGPiJUx7kcHeK7apAH1xB4DnfuPLSC1GjWptb31A22wjWy/75SJk8
0FoyYKPj5RqiQF+5CcSLRwTJEEi+9ggM8mUJiFNUOtfZgATgmCyEKG4fL1N4iyrj
fBha11/EO3LcH4t0rj5i8SkT+w8A0bgpOliLhnKpFQMy+cRewkzNIS2ynGlHqnKA
biuBEr1ji0iHNHczTMuqSYwraVHis+098D+1me5+9SaDp8yEIKgVuTUAuQINBGOV
dwcBEADKRVXM2aPWTzbIFu/dVFuaOsJ653dZyDvkuK3N+6tkxM/ChhwrsaOTcH32
drei59OASOeKW2qYNe2+2tIT5Gt+xxZC9vJ+FcjHcdArAJt0BH1LHSuscCldkrnG
HlXK1dbqXDeD3Vw+7LtSO/wOAllxSRtOO8ydGfPZSWYkBIgKu4IbxKIpwtLJvtGu
mqP6HKgoFgijNcgjzssyV5Xka79vUkZ2M4jEfqtlNMfcYPV5ehjMFJhcGyXPZzkV
byx+321Ov3bvBIKAGK4JRThWRv00qJUhlkUjImr89CUg/4vqxDeGiE+FnwXvi/Vs
tQJqzcYgDvsypsx0LtyUsQ53K/svoXHfltIKsNdBaCPY1i3C+5EfumtIjo7iUl0q
Katpdw2n4j8bQhZq+AhkIcwRzOnuP7/zTXdxdF6VWyekUKYe5ZH738/Ktpb1JR4X
sydKdcV5oX3/Qh43VTIZgJs+fopgQF5NpqLbTXym9KRRHp9cWNyv1DwOIPqD7Eo+
PeTLLyIPXiDAnAt/89EhFDFh/7Lcsicz6n6cnxsGXk3CI/b4NqPkZxr5nC1WAPxB
k6D5PdOZL/3Cu96MvG2cjgdMzIO0/T2loC1DtLKo6qNDMN5JxckoN6EV5XIpT0L3
z3V9Cb8C6XPQ1pa9ftRpAlydPJVroCXPegiULqSkW9SGwtKFFwARAQABiQI8BBgB
CgAmFiEEC+MydddMlTx5+BEH2a0qGAV0dMsFAmOVdwcCGwwFCQICKQAACgkQ2a0q
GAV0dMsMLQ/8CA5hHB3RZchUU6JlAY23itrs3GSIZJIC+fJXOt1D5XuYidhQb5mE
vtK0Eud7FRLHHJ+Sn5DsE68ipZb1m5dCM7oqn2sMQC3H1qX2SR80zEpwx34F7zjs
hTEK7qkQwBwK+zzQtAp209LBBdmRc2nfDPXy6rZF1MeJoBAjRieAlaoO+SmPLlM7
/wZkcBH+fOxU+f4gCHneTIxQdlRQ1/RgAXL002x8QmSMZ8Zd3LNeUsU9JQKH2drn
lOpFmFmUlxXmhDP+MpjycLNppldAJGyYIS1wp/TMd51+jU2WfR2q267vkc1t/x4N
```

```
w2XdCfb5KPD2nz9JdTVrYMl++Aqr04I808V056q0V83HMyu34XAtruItKaz7V13M
sou0sKaC4pGmQixRYVJjsfpkuU47YBchWQTcZzu4gMJM33E3AvbD6FmhZokH+quR
CGMxvlkKZ3I/NJsZdx1jj+qBY/4WSUWLHinjJLycy06PO6xXTOgrDKy8BE0envml
jNG7TxYpda11QAjTo7MtG8U1fDiRH8sZ2Jso75wbwdJHYmlRA3VYcYEqsywF+JoF
2uPf1ejP7szK/p9/wNSXZOFen1ZvEuXBSF8aFGrd3AeMRmk/Tlg96NTT6+nkvVaN
BLCZUZfNUhuvH0vkLZNn19u0+vGBuAGt8zH2cVLFbhS7U7kG0QvnyaSJAjwEGAEK
ACYCGwwWIQQL4zJ110yVPHn4EQfZrSoYBXR0ywUCZYXLqgUJA/J9aAAKCRDZrSoY
BXR0y6DtEACbExPX5JXm+2MzxLj/Rid48fDxnVpu5/vFDXa9uJEuoDl1VHz2a1mu
UqNtYXCMGW+D2Q6h0lUkJ0XIioUpxu4KZWDzRmePhVmy6/5gUWGq45FRS1Lgj3sU
iI8VdSkhiZ1rPWE1QCmQM++RqQjC+ow+m4gjkAkPOsKjnVr2SGUfGL7q68UeuAAQ
dK427GhvHDTlF9XMAH3S8LYX+uHUvtpt5ajRgx5D+XjS9ESMQuYF2BKdJb5pTB92
bjuVq3x+9z0w4PPW8V3roaxZkhMH+MVputN6IvP9qkL0ff+429KPre9TULlq1iBT
jWVloGQVBrKPrsk914GOGKihkd89kMyh2JyejO0r0mKaku0bXMXAlxdBxjXxEvHA
ILSlaRbW7UsF16fDvKC8o5lSDvzY1KWyzhnRSLGq7HsyxVfX9n6metyd+IclEoPC
62FVdXwOQyVKXm21+IS6XZNDDLYBuNwcCiBpSU6S+UZEP7kFN2FtpGoq8u6PtYpg
w9E0c0MbXY1TiOb55UzXHyWSCHy8eHawAQNdjr6V93Xz1etkfvAQJSRU+N9AhugC
EiSAaiURb7opJp2RlLxB5jlLPxS222l0z5CnO7UdliMJY0bzFfkJPOHFnF+mHITL
JTLogzNZrZUGYoN+FhxkhPswlp1wLJSB5UsKMe6n3TtCs9l53EmyAIkCPAQYAQoA
JgIbDBYhBAvjMnXXTJU8efgRB9mtKhgFdHTLBQJnhEEuBQkF0/ICAAoJENmtKhgF
dHTLJtUP/1dPcTrrUm1lOOCkbq3ZxirJOegxZal7YxmCagz6zg6V9zPCA39jLkyD
dsnzzL/fOGwGzgPUS+xGhlZUFFvUFj1ETLGShBUJY4X8USTvSaBg2CO7kQ50hIul
o1b4FJOToiIdChCOIxHGiws73iBHLMK1Q0gJ/u5xr3sD/Ea8e6jFDbywJbcYjMnx
l53mr0bN7H7rM3W/S002PJQlNMa7JWl6673wpGkW7JBYt0t9SPtWQf3sLgIR6n3N
d3kQYz8EDmpyRXqQMz+BheNX1UDfRrbLAEwg/nVejhYWI31iWziHD79u+8ArxiBb
nDPV0Y25AiGBUBOVvtTv2nLdzm49bAfdAvnFToAp4N+2Knzm2CxdfUROPmuzVAIf
xsR4/vE8VMr762llsnzakzA4xzEoTQ4xtKksxV+738lKZnwH8/umne/GpLPSzH/v
OohpLwYVxbO3M1b+D1lmFdflkoTVNmPcjGh986VlGkRHQdOxymy72uGNYnKllcfs
+sbNz77Km03ov5qF4mZO6IaWwZtIbSZZIttgEWKxl0iusOUULQmaAVtAxI+STQY5
Cul2wFt1RbgANSecC0ts9HiEeWnT/v0sUFG06vmRYjhnQT9YP+/N3u8xHcgNGHwN
ilPTnS87qVIsf8fiWHMZq2V53UjDm3dCIljocF5YGq2ySTEXjjkYiQI8BBgBCgAm
AhsMFiEEC+MydddMlTx5+BEH2a0qGAV0dMsFAmluhHIFCQmhpDsACgkQ2a0qGAV0
dMs5ag//V7mahuI9VikX1lG599GSjm1cXeDrZmGtamz9hYE7EzGlyxf5WQn83Sxu
2kNe9UbaLcIpKzZ9CWcb7NfC6odUIzJsO21qSKNuoP7FV9472JTNFMhaj1+o1P8b
v1nGOU4H9IH/y0Wqkuteef3t4le0iCtePMU3vXgfUFAmm/VF/tgmJQb2hLkXFNCQ
QwK//jjm9QHajaU2wEpvskarsRGfGBintBbUqUUxyPgirqAC8dFAWrjefmGePWEW
JfRLql39II+xbjEzADBB8yqnxLuaUQfVF7t2oAOfp09dP++bCua7FO1WfuFoa1Yw
um84/XszGgkxDRFkBxabpMCurPWgyhkGto4TqKdcWTMl4S1rTxt4Bm/6fqMn+04z
/AiXgU/iIbEKhvQUxsTxyNBLPFIRD7VmrqrOr3wkHgGHJgP0656ABq5J+T4mtFhX
uL0U9nGSm5lV9Hl1ana+Kcs4DqzgQO3QJk/SoulBDZ6at0pK2Y016JrvY51fYpx6
a/IOaXE2JRi8itVlpciDTjSOJs4eNlUx0C3b/LdzU5LZqHtBea1xWxlKPn0VFjYr
YNML6o5B6AL05AcySZj8kNZTWE2ZfOR2usLdiB8b+u2F7WGXZBiQYSnr75WsN94S
nYwO46v5SlzGqTwEN/UBfTkKPklVNgeOMn7fgjziEtMmtBlb7ws=
=ijsc
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.2. Γραμματέας της Ομάδας Core <core-secretary@FreeBSD.org>

```
pub   rsa4096/4D632518C3546B05 2024-02-17 [SC] [expires: 2028-02-08]
      Key fingerprint = 1A23 6A92 528D 00DD 7965  76FE 4D63 2518 C354 6B05
```

```
uid                             FreeBSD Core Team Secretary <core-
secretary@FreeBSD.org>
sub   rsa4096/CABFDE12CA516ED2 2024-02-17 [E] [expires: 2028-02-08]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGXQ1o8BEAC+Rcg8cmVxuP17Vu+q5KgCx/XiulQuqKXAqqBlYCH2jqk6DINP
yFrREGBhzd/qNmlAYEahQ4Zgl0bUZNTrZVDyzicOvPP0jH+KSTQwRs7NOawEdlVO
cyHrwDCPEqf5ZzD4NhfTriEOw+j0pEH/onitUGvoQRtx15xWyaJQxDEBMTYMLewE
86D1bltwnTNczE3UZb7oQLJXkAX5hcLtou70XJGgZITvJkK+kp/xot2eFjnqRz/u
WeXnKhYAmC07EKwZ1uw047eHKwMMRBYqzApLwoQtfE430Kxf2q8de64x8zDbi6YM
1J4r8OAxOtHVyfJ0j7Q23DEZz0VVb4b1Tx5OG2Re/KSNvqI0awJO4TcRmOR88OyY
dzyXgnX6Sa7GVQY1FXvn7vtFuDAt7egZOzeomSHL9bdX07LTQ4UtM88EV9wm3q4q
smoatV9jsvPQ1zxCU3aQD/5eWTJH2/kz1LIuBL/Qi5XQpJn91lBtUWJrCgkHWPGu
f//rnnXmsG7DAChW+yZ7cFO8lfNa8sFhPqSxCYphWmJTrvadyQtDngB8JakWdnmK
pfGS6y5lel+181vw38ZZKt04AKM+nDY8051lBM7Q9Q6kTLI33UZeImndx5xYukVD
kV6aQ31HYfEark15c7iEz+OAcwFnM2ntXMt7kKGd40CqzusiPcQkPqPbAQARAQAB
tDhGcmVlQlNEIENvcmUgVGVhbSBTZWNyZXRhcnkgPGNvcmUtc2VjcmV0YXJ5QEZy
ZWVCU0Qub3JnPokCVwQTAQoAQQIbAwgLCQ0IDAcLAwUVCgkICwUWAwIBAAIeBQIX
gBYhBBojapJSjQDdeWV2/k1jJRjDVGsFBQJnp8PiBQkHeofTAAoJEE1jJRjDVGsF
GMIQALhj+mNpH8OmTFeihQ6t9P8un3llz6Wmqe/Q+ULWeqJvV/uC1J5T9fnoGhwF
MgECuguXYJtoYQ16KXnsSOs1tcqMOK9GtEtFJTGe2DtfLiBednwUvu9j3HmTlwLN
M+7rqkiC0HCg2qSjcMjxbVbA5BSgNkgfyTSO2YdjfaZ+ceiHwo/qa5xWE6i2dMR1
PLGMMHTeELdtdSH6VR9/3h0qt3qzwdMBRCVAQHbim7CqwjUH9jg+IOySXl81jNoB
xuVZR3pKshyY4Oxo1dK+W86Uiff/+c4jCAxokGWIR7C4MkZZWUQqV7920gkZFC/5
qzpT1A1/sFUg8HfFTr0vCoPSVFWn2+Tto3vr78DICVaAf02aYAFlyKK18BMCoHkS
hDDO+/JQZmvHOIgEYK+T2WN1c9gm9IDJzGZuH0X2C/vkREnJKkccJfB4pXuN10wt
fqyP9fn8h6+/t+sv3qNLm4d8fkmLXofulG3WB4i/F+Hip2rjPvvBCF7zl4xy6cJ2
xVY5HUOBTqmIwVhYwUpXaqNoWa/qJBLTuot3z7ciKmKX6Lq+Dze5dzhrPNl/CalC
HBf3miHRK3TZbYLooG3bcEWgxU2BnBi3vl5NpCoUOKkPYRlALXi2TyHmPxO7oT4e
mIzS6BgnXOqO+AXvbKKfayuSePdBqkNMK/SMC4Dylkf6Xj25iQIzBBABCgAdFiEE
EBpxaxYrAOVb7eoFrbv4YQo3ibcFAmbu7x4ACgkQrbv4YQo3ibcr5A//TIcbD/EW
YJz0zrUQdc9xG3UNfU6uHmQzAuUy5ginevyqv0TSso5qvSkOHvdxbi41rfMiB2RJ
V3q0n0PSvHFld89fOTZUMZXaPvozCiBYWScrt+KA/2pq3K8mUumHS+IFtpHLL2Tu
+gI8XCHUFxO9HUThM/rFlIyEdzoctgmqQ7IG4uZG+o2J3w09llhDAUe0vraJK1On
p9yFACnRrhqvl41JeUWcv9MH9JcwHUqtUo9WLTCIb+hkByTOyRfHBYpYw//bdXdf
6rkCwKVWpyMDbk61zq2VsS1kqbP9IH/A8CsBnA6mg+zPq2i7HIFw8Swj4OGJcIvG
a9ubUYJRjDhX/vBpNrtncANZ88FQmA+Maq0vu0LS5IIGyIKkvd1fKIsyvBDDa9kE
nfCW0XMkJA0Gf+kxdB+elXQHBwKO2sr5BiKnJT5lJq3Yu9fxxGBnf93yiN4E9bmF
gG7cZxpyb1Bp76TJhLcANyybOTjCtiNRrgqeaSx9/6hSPfPigGXIne0H2lmJO6oq
jUrsYmFiWvU9sc7AcPVw/eHG8FgW35TuwKX71z8w994iaahUPNcSVyXOUD+QNROv
HhGUXrc81t613rivh22N0NZpNubVatq43KV7+/bnPyWBIi1Awh3vIFsNNSQSrYxF
lUuQaAHQXTeZMZ/7npE4t86seMt0T7BGn765Ag0EZdDWjwEQAL3VwFifpnRCYzQ4
VZ1dAjp8w542iRprqeA+C3tvNbk2OvKpN3DIc49l2bgNZ/VI7/T58lEKrFsgLK4w
AWtv18OV7xuh0AuOblmq5MvcPrUelkPj5HA7M6Ng/rAubuHfwdP/IjIrzzY6+XDh
fP9N5KIv9VRJYT23BbvLPeit4J4tQEB/NpxL3L6zI75qq4R3T/EkHP6Y9Buup9Lr
isJlcxkSK+CyORCgTpEz6fWsXiTDgS7cTaQ969XCygBpj4wRQzwkBdokxo1wsiFt
4zLt07/PrPYjeHltTDkrF9XDNhLNJ5GliHnd01oHg1j5/n+9Osvh1maoFwuBxXTN
nTZ2P+7RKLBaVQVSkUa5KJbXoM3v7bMbXM5aLs2XjglrAzrZOV+Y7zOu5UYQdpXd
7x8XAEtEozRJzt7dosQIhKx9h4LlltFFulDUpf5VCvcUEoAzMbiX0aju9n5Rwsql
```

```
DHatU9Mm3W8OdFXj1foIXZD+VX2Jp9DgxPLoAJ0CWhPXJ8f+WFSJZCjWoPJEJKWY
0EOxiXyAuvAyniAZAC/eKZkfGckXmu7edRgYbRTTwPmZ/axa/k9aHsHLwmbxuZo/
xxQXzqU70EleHZ31A3mOqsC1epjN6dn4AFKgvVesP/K/fbvSsfsfiABS2A/68ne4
zJG73Tnk4L6J79vrXc2iMJbmdg3ZABEBAAGJAjwEGAEKACYCGwwWIQQaI2qSUo0A
3Xlldv5NYyUYw1RrBQUCZ6fEFQUJB3qIBgAKCRBNYyUYw1RrBQd9EACMVckxzy4w
aUGlERguJ+kslS8MkMjNqnfDPLRDVxbUxNvbbhw7/u9blM65DCGCeNLc2n4oiu5C
E3I095AKmvq/0dOa81mEEdZkC1CVc64bXWbEyz5AtSHUpgdxRso6C+YopndSiz1T
WcIagQRXfWaw3FBWPooA87gmibmSmCegCtqx+uyc5QxX2eFI8mRK7vlfnGpYKHs0
D1/yUSGQOwoNRJ5FYm+ynfDE3FzHEQL7lv1vpv1k3xNKfBziMMg4IMEBKNHV4VKN
qJpa8UCodeTGSWQdNnCeCWPsxz5oQjCcVH9Z3e8sMpWLHhRcBZzSwXUOws2GbRMH
xHwrfrpHJcrBhe64pgfGOvZLUJ9BDs+8egTHsqRFacipbtTR+hhVhuJEHDaQQWuM
8IRHj9HIuTAczET8JTDHTMIoo8DZdOtiW/YgqCDwYghkI77d12oNQqYoeJ2HiqbK
cGzwCpsR0A+p/iOAxJG13tsxqZV8TQ8iTokWG6ACtZ7sfeWEhxqMbUKUMgogZn0I
3n1kV+tUZC6BQrIYI7TiKg95wLZsIydeoIsQoNZwvyKAXfVmQ62YjIX8njZwN+07
8/ipUPJxCYa8zL8BZyDmoFJqa3y9z+11+vtiZ9t+aTwGvjpHDwyeCJco7go9cU3m
GRFZYciqIoG4n3tl8Pob15vFlVqk47rRqg==
=8TzT
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.3. Γραμματέας Ομάδας Διαχείρισης των Ports <portmgr-secretary@FreeBSD.org>

```
pub   ed25519/E3C401F60D709D59 2023-03-06 [SC] [expires: 2027-03-05]
      Key fingerprint = BED4 A1D3 6555 B681 2E9F  ABDA E3C4 01F6 0D70 9D59
uid                           FreeBSD Ports Management Team Secretary <portmgr-
secretary@FreeBSD.org>
sub   cv25519/2C92B55E27A641C3 2023-03-06 [E] [expires: 2027-03-05]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZAXJvxYJKwYBBAHaRw8BAQdASFAC20WL3R1T6uNyGMZbfJCxDkcP4C5vi3Op
tcZ2fbq0R0ZyZWVCU0QgUG9ydHMgTWFuYWdlbWVudCBUZWFtIFNlY3JldGFyeSA8
cG9ydG1nci1zZWNyZXRhcnlARnJlZUJTRC5vcmc+iJYEExYKAD4WIQS+1KHTZVW2
gS6fq9rjxAH2DXCdWQUCZAXJvwIbAwUJB4TOAAULCQgHAwUVCgkICwUWAwIBAAIe
BQIXgAAKCRDjxAH2DXCdWYN1AP43TjyfZtZ3DLYT++g0+SuPsoO/3yWVybA+UmFL
zb8MngEA+LLNUfvEwCuXS/soh+ww5bpfmi3UUmeGiQEAXug3iA+JATMEEAEKAB0W
IQT7N0XIbxXo7ayBMvzYKU7Du8TX1QUCZAXLkwAKCRDYKU7Du8TX1XHMB/9R1MX4
6zMgpKqPPt76GOI+eGEdBK6bY8aJZjQGdqTh9f6VtXVoTGIG7cvhc9X8tDBoB0PT
2KZWheF51AV1+NHU4HwLAQ1BMebrFvWSfkw4xg4fBGwDhz9/GN85No+Js772V5ey
8lRiL6meRVWxMlLyWcxGd8JjcC5yX/iAUQ3SBGCLqW7unWjjg7CTd+AMBwcqPGrv
ax8q6eFVguJcHJAjMnKf6HAy4cpK3s+uMoUBCGnszSN12B3ysKfyC4pNO/pix5tA
Q5v8aRqTeFPh5zmNhWo0KGPzplTPqRQSHDl7GDQC8Ru3MhzFkeWzHsexjZVwS6W2
DPcYpuuAsA0XOZIZiQIzBBABCgAdFiEEEBpxaxYrAOVb7eoFrbv4YQo3ibcFAmQF
0u0ACgkQrbv4YQo3ibccwg/9F2Xuic3nhKxRbB3mJeDo6SYQETa/Gh1qQ34+8zlt
8UMazOx67gnYQfy+pXjro6eQ2up0a4eUYezcNOudqAQD21nRz3HA6EQVNcE/TzEA
xl5CJntTaLOt7S+EDXFW5BuQIvhhoMGgm8+WNVgA0EJ7tfL0OcYBSvr19fqwChEn
9c14cSk6mgHSsleP5NvskYN053pxHwy0LTSb8YBBv52th37t/CRFC1363rS5q+D7
JixFopd1O5pKpA5ipvE4gGgRjPtwjx0SjjepwK/3fuhEJQQyKzTIKlMfu2Dj/iR2
```

```
Li1Sfccau5LQXOj9fUITU3u1YG7yrm8VGzT7ao4d+KRwgMLjd2pLqiGIbbJwGBiP
FRmtilWQoeIlmSlFX4obAA517DOK0pW1mH8+eEn4EJd3SekT3yzFyKTASv0J48Z8
3F928xg+eZvHxVC0t1J+J5IG0gt3EEncuWKIPQGR7PiQbti6R3FQVTz6WfMWOebP
Qi0E9F/Aqakr6Vj2sKGrDq+ebpaF5G8Yw1YrUl2IDiPzkCegp3ZbI0wh11Xvzhi8
LXPQGK4jBQas4G8cegfitzmtdGRHYrbMv0R9I4mvaL+WlOuD2AvyVG28lguqVhnN
AZP+ohdquYyX2CNCVvbKWAtXo6Ur0vWG8BL8m6defAtEkIwVBALaOHQOSI3aNUz4
lwy4OARkBcm/EgorBgEEAZdVAQUBAQdAsefmSfxEOdOr02+K/6noYCuJ1FeAWVz6
jFYQ+9w6jggDAQgHiH4EGBYKACYWIQS+1KHTZVW2gS6fq9rjxAH2DXCdWQUCZAXJ
vwIbDAUJB4TOAAAKCRDjxAH2DXCdWRl4AP9h5ot212BK29S6ZcMBhHvmtF5PG1oD
c7LnZycSRmbFiwEAndCMpAGOhDW8iVgDd0wLQq/ZMPe+xccfG1b3zFH2EgE=
=iiAT
-----END PGP PUBLIC KEY BLOCK-----
```

D.1.4. <doceng-secretary@FreeBSD.org>

```
pub   rsa2048/E1C03580AEB45E58 2019-10-31 [SC] [expires: 2022-10-30]
      Key fingerprint = F24D 7B32 B864 625E 5541  A0E4 E1C0 3580 AEB4 5E58
uid                           FreeBSD Doceng Team Secretary <doceng-
secretary@freebsd.org>
sub   rsa2048/9EA8D713509472FC 2019-10-31 [E] [expires: 2022-10-30]
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQENBF27FFcBCADeoSsIgyQUY8vREwkTikwFFlNg31MVy5s/Nq1cNK1PRfRMnprS
yfB62KqbYuz16bmQKaA9zHN4FGfiTvR6tl66LVHm1s/5HPiLv8sP14GsruLro9zN
v72dO7a9i68bMw+jarPOnu9dGiDFEI0dACOkdCGEYKEUapQeNpmWRrQ46BeXyFwF
JcNx76bJJUkwk6fWC0W63D762e6lCEX6ndoaPjjLBnFvtx13heNGUc8RukBwe2mA
U5pSGHj47J05bdWiRSwZaXa8PcW+20zTWaP755w7zWe4h60GANY7OsT9nuOqsioJ
QonxTrJuZweKRV8fNQ1EfDws3HZr7/7iXvO3ABEBAAG0PEZyZWVCU0QgRG9jZW5n
IFRlYW0gU2VjcmV0YXJ5IDxkb2Nlbmctc2VjcmV0YXJ5QGZyZWVic2Qub3JnPokB
VAQTAQoAPhYhBPJNezK4ZGJeVUGg5OHANYCutF5YBQJduxRXAhsDBQkFo5qABQsJ
CAcDBRUKCQgLBRYDAgEAAh4BAheAAAoJEOHANYCutF5YB2IIALw+EPYmOz9qlqIn
oTFmk/5MrcdzC5iLEfxubbF6TopDWsWPiOh5mAuvfEmROSGf6ctvdYe9UtQV3VNY
KeeyskeFrIBOFo2KG/dFqKPAWef6IfhbW3HWDWo5uOBg01jHzQ/pB1n6SMKiXfsM
idL9wN+UQKxF3Y7S/bVrZTV0isRUolO9+8kQeSYT/NMojVM0H2fWrTP/TaNEW4fY
JBDAl5hsktzdl8sdbNqdC0GiX3xb4GvgVzGGQELagsxjfuXk6PfOyn6Wx2d+yRcI
FrKojmhihBp5VGFQkntBIXQkaW0xhW+WBGxwXdaAl0drQlZ3W+edgdOl705x73kf
Uw3Fh2a5AQ0EXbsUVwEIANEPAsltM4vFj2pi5xEuHEcZIrIX/ZJhoaBtZkqvkB+H
4pu3/eQHK5hg0Dw12ugffPMz8mi57iGNI9TXd8ZYMJxAdvEZSDHCKZTX9G+FcxWa
/AzKNiG25uSISzz7rMB/lV1gofCdGtpHFRFTiNxFcoacugTdlYDiscgJZMJSg/hC
GXBdEKXR5WRAgAGandcL8llCToOt1lZEOkd5vJM861w6evgDhAZ2HGhRuG8/NDxG
r4UtlnYGUCFof/Q4oPNbDJzmZXF+8OQyTNcEpVD3leEOWG1Uv5XWS2XKVHcHZZ++
ISo/B5Q6Oi3SJFCVV9f+g09YF+PgfP/mVMBgif2fT20AEQEAAYkBPAQYAQoAJhYh
BPJNezK4ZGJeVUGg5OHANYCutF5YBQJduxRXAhsMBQkFo5qAAAoJEOHANYCutF5Y
kecIAMTh2VHQqjXHTszQMsy3NjiTVVITI3z+pzY0u2EYmLytXQ2pZMzLHMcklmub
5po0X4EvL6bZiJcLMI2mSrOs0Gp8P3hyMI40IkqoLMp7VA2LFlPgIJ7K5W4oVwf8
khY6lw7qg2l69APm/MM3xAyiL4p6MU8tpvWg5AncZ6lxyy27rxVflzEtCrKQuG/a
oVaOlMjH3uxvOK6IIxlhvWD0nKs/e2h2HIAZ+ILE6ytS5ZEg2GXuigoQZdEnv71L
```

```
xyvE9JANwGZLkDxnS5pgN2ikfkQYlFpJEkrNTQleCOHIIIp8vgJngEaP51xOIbQM
CiG/y3cmKQ/ZfH7BBvlZVtZKQsI=
=MQKT
-----END PGP PUBLIC KEY BLOCK-----
```