Network Working Group
Request for Comments: 2477
Category: Informational

B. Aboba
G. Zorn
Microsoft Corporation

January 1999

Criteria for Evaluating Roaming Protocols

Status of this Memo

Copyright Notice

1. Abstract

This document describes requirements for the provisioning of "roaming capability" for dialup Internet users. "Roaming capability" is defined as the ability to use multiple Internet service providers (ISPs), while maintaining a formal, customer-vendor relationship with only one.

2. Introduction

Operational roaming services are currently providing worldwide roaming capabilities, and these services continue to grow in popularity [1]. Interested parties have included:

Regional Internet Service Providers (ISPs) operating within a particular state or province, looking to combine their efforts with those of other regional providers to offer services over a wider area.

National ISPs wishing to combine their operations with those of one or more ISPs in another nation to provide greater coverage in a group of countries or on a continent.

Businesses desiring to offer their employees a comprehensive package of dialup services on a global basis. Those services can include Internet access as well as secure access to corporate intranets via a Virtual Private Network (VPN).

This document provides an architectural framework for the provisioning of roaming capabilities, as well as describing the requirements that must be met by elements of the architecture.

2.1. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "optional", "recommended", "SHOULD", and "SHOULD NOT", are to be interpreted as described in [4].

Please note that the requirements specified in this document are to be used in evaluating protocol submissions. As such, the requirements language refers to capabilities of these protocols; the protocol documents will specify whether these features are required, recommended, or optional for use in roaming. For example, requiring that a protocol support confidentiality is NOT the same thing as requiring that all protocol traffic be encrypted.

A protocol submission is not compliant if it fails to satisfy one or more of the must or must not requirements for the capabilities that it implements. A protocol submission that satisfies all the must, must not, should and should not requirements for its capabilities is said to be "unconditionally compliant"; one that satisfies all the must and must not requirements but not all the should or should not requirements for its protocols is said to be "conditionally compliant."

2.2. Terminology

This document frequently uses the following terms:

phone book
: This is a database or document containing data pertaining to dialup access, including phone numbers and any associated attributes.

phone book server
: This is a server that maintains the latest version of the phone book. Clients communicate with phone book servers in order to keep their phone books up to date.

Network Access Server
: The Network Access Server (NAS) is the device that clients dial in order to get access to the network.

Authentication server
: This is a server which provides for authentication/authorization within the roaming architecture.

Accounting server
This is a server which provides for accounting within the roaming architecture.

Authentication proxy
Authentication proxies may be deployed within the roaming architecture for several purposes, including authentication forwarding, policy implementation, shared secret management, and attribute editing. To the NAS, the authentication proxy appears to act as an authentication server; to the authentication server, the proxy appears to act as an authentication client.

Accounting proxy
Accounting proxies may be deployed within the roaming architecture for several purposes, including accounting forwarding, reliability improvement, auditing, and "pseudo-transactional" capability. To the NAS, the accounting proxy appears to act as an accounting server; to the accounting server, the proxy appears to act as an accounting client.

Network Access Identifier
In order to provide for the routing of authentication and accounting packets, user name MAY contain structure. This structure provides a means by which the authentication or accounting proxies will locate the authentication or accounting server that is to receive the request.

3. Architectural framework

The roaming architecture consists of three major subsystems:

Phone book Subsystem
Authentication Subsystem
Accounting Subsystem

The phone book subsystem is concerned with the maintenance and updating of the user phone book. The phone book provides the user with information on the location and phone numbers of Points of Presence (POPs) that are roaming enabled. The function of the authentication subsystem is to provide authorized users with access to the POPs in the phonebook, and to deny access to unauthorized users. The goal of the accounting subsystem is to provide information on the resources utilized during the user’s session.

3.1. Phone Book Subsystem

The phone book subsystem provides for the following:

Phone number presentation
Phone number exchange
Phone book compilation
Phone book update

Phone number presentation
Phone number presentation involves the display of available phone numbers to the user, and culminates in the choosing of a number. Since the user interface and sequence of events involved in phone number presentation is a function of the connection management software being used, it is likely that individual vendors will take different approaches to the problem. These differences can include variances in the format of the client phone books, varying approaches to presentation, etc. There is no inherent problem with this. As a result, phone number presentation need not be standardized.

Phone number exchange
Phone number exchange involves propagation of phone number changes between providers in a roaming association. Current roaming implementations do not provide for complete automation of the phone number exchange process [1]. As a result, phone number exchange need not be standardized at this time.

Phone book compilation
Once an ISP's phone book server has received its updates it needs to compile a new phone book and propagate this phone book to all the phone book servers operated by that ISP. Given that the compilation process does not affect protocol interoperability, it need not be standardized.

Phone book update
Once the phone book is compiled, it needs to be propagated to users. Standardization of the phone book update process allows for providers to update user phone books, independent of their client software or operating system.

3.2. Authentication Subsystem

The authentication subsystem provides for the following:

Connection management
Authentication
NAS Configuration/Authorization
Address Assignment/Routing
Security

Connection management
: In order to be able to use the POPs of the local provider, it is first necessary to bring up a connection.

Identification
: Authentication consists of two parts: the claim of identity (or identification) and the proof of the claim (or verification). As part of the authentication process, users identify themselves to the Network Access Server (NAS) in a manner that allows the authentication request to be routed its home destination.

Authentication
: Authentication is typically required prior to allowing access to the network. CHAP [8] and PAP [9] are the two authentication protocols most commonly used within the PPP [10] framework today. Some groups of users are requiring different forms of proof of identity (e.g., token or smart cards, Kerberos credentials, etc.) for special purposes (such as acquiring access to corporate intranets). The Extensible Authentication Protocol (EAP) [7] was created in order to provide a general mechanism for support of these methods.

NAS configuration/authorization
: In order to set up the session, authorization parameters need to be sent to from the home authentication server to the local ISP's NAS.

Address assignment/routing
: If it is desired that the user be able to communicate with the rest of the Internet, then the session will be assigned a routable IP address by the NAS.

Security
: In the process of authenticating and authorizing the user session, it may be desirable to provide protection against a variety of security threats.

3.3. Accounting Subsystem

The function of the accounting subsystem is to enable the participants in the roaming consortium to keep track of what resources are used during a session. Relevant information includes how long the user was connected to the service, connection speed, port type, etc.

4. Roaming Requirements

4.1. Phonebook requirements

4.1.1. Phone book update protocol

Portability
The update protocol MUST allow for updating of clients on a range of platforms and operating systems. Therefore the update mechanism MUST NOT impose any operating system-specific requirements.

Authentication
The client MUST be able to determine the authenticity of the server sending the phone book update. The server MAY also be able to authenticate the client.

Versioning
The update protocol MUST provide for updating of the phone book from an arbitrary previous version to the latest available version.

Integrity Checking
The client MUST be able to determine the integrity of the received update before applying it, and MUST be able to determine the integrity of the newly produced phone book after updating it.

Light weight transfers
Since the client may be a low-end machine or internet appliance, the update protocol MUST be lightweight.

Language support
The phone book update mechanism MUST support the ability to request that the phone book be transmitted in a particular language and character set. For example, if the customer has a Russian language software package, then the propagation and update protocols MUST provide a mechanism for the user to request a Russian language phone book.

4.1.2. Phone book format

Phone number attributes
The phone book format MUST support phone number attributes commonly used by Internet service providers. These attributes are required in order to provide users with information on the capabilities of the available phone numbers.

Provider attributes
In addition to providing information relating to a given phone number, the phone book MUST provide information on the individual

roaming consortium members. These attributes are required in order to provide users with information about the individual providers in the roaming consortium.

Service attributes
In addition to providing information relating to a given phone number, and service provider, the phone book MUST provide information relevant to configuration of the service. These attributes are necessary to provide the client with information relating to the operation of the service.

Extensibility
Since it will frequently be necessary to add phone book attributes, the phone book format MUST support the addition of phone number, provider and service attributes without modification to the update protocol. Registration of new phone book attributes will be handled by IANA. The attribute space MUST be sufficiently large to accomodate growth.

Compactness
Since phone book will typically be frequently updated, the phone book format MUST be compact so as to minimize the bandwidth used in updating it.

4.2. Authentication requirements

4.2.1. Connection Management

Given the current popularity and near ubiquity of PPP, a roaming standard MUST provide support for PPP and IP. A roaming standard MAY provide support for other framing protocols such as SLIP. However, SLIP support is expected to prove difficult since SLIP does not support negotiation of connection parameters and lacks support for protocols other than IP.

A roaming standard MAY provide support for non-IP protocols (e.g., IPX or AppleTalk) since these may be useful for the provision of corporate intranet access via the Internet. Since it is intended that the client will begin PPP negotiation immediately on connection, support for scripting SHOULD NOT be part of a roaming standard.

4.2.2. Identification

A roaming standard MUST provide a standardized format for the userID and realm presented to the NAS.

4.2.3. Verification of Identity

Authentication types
: A roaming standard MUST support CHAP, and SHOULD support EAP. Due to security concerns, PAP authentication SHOULD NOT be supported. A possible exception is where PAP is used to support a one time password or token.

Scalability
: A roaming standard, once available, is likely to be widely deployed on the Internet. A roaming standard MUST therefore provide sufficient scalability to allow for the formation of roaming associations with thousands of ISP members.

RADIUS Support
: Given the current popularity and near ubiquity of RADIUS [2,3] as an authentication, authorization and accounting solution, a roaming standard MUST be able to incorporate RADIUS-enabled devices within the roaming architecture. It is expected that this will be accomplished by development of gateways between RADIUS and the roaming standard authentication, authorization, and accounting protocol.

4.2.4. NAS Configuration/Authorization

In order to ensure compatibility with the NAS or the local network, authentication/authorization proxies often will add, delete, or modify attributes returned by the home authentication server. In addition, an authentication proxy will often carry out resource management and policy functions. As a result, a roaming standard MUST support the ability of proxies to perform attribute editing and implement policy.

4.2.5. Address assignment/routing

A roaming standard MUST support dynamic address assignment. Static address assignment MAY be supported, most likely via layer 2 or layer 3 tunneling.

Layer 2 tunneling protocols
: Layer-2 tunneling protocols, such as PPTP, L2F, or L2TP, hold great promise for the implementation of Virtual Private Networks as a means for inexpensive access to remote networks. Therefore proxy implementations MUST NOT preclude use of layer 2 tunneling.

Layer 3 tunneling protocols
: Layer-3 tunneling protocols as embodied in Mobile IP [5], hold great promise for providing "live", transparent mobility on the

part of mobile nodes on the Internet. Therefore, a roaming standard MUST NOT preclude the provisioning of Mobile IP Foreign Agents or other Mobile IP functionality on the part of service providers.

4.2.6. Security

Security analysis
A roaming standard MUST include a thorough security analysis, including a description of security threats and countermeasures. This includes specification of mechanisms for fraud prevention and detection.

Hop by hop security
A roaming standard MUST provide for hop-by-hop integrity protection and confidentiality. This MAY be accomplished through support of network layer security (IPSEC) [6].

End-to-end security
As policy implementation and attribute editing are common in roaming systems, proxies may need to modify packets in transit between a local NAS and the home server. In order to permit authorized modifications while at the same time guarding against attacks by rogue proxies, it is necessary for a roaming standard to support data object security. As a result, a roaming standard MUST provide end-to-end confidentiality and integrity protection on an attribute-by-attribute basis. However, non-repudiation is NOT a requirement for a roaming standard.

4.3. Accounting requirements

Real-time accounting
In today's roaming implementations, real-time accounting is a practical necessity in order to support fraud detection and risk management. As a result, a roaming standard MUST provide support for real-time accounting.

Accounting record formats
Today there is no proposed standard for NAS accounting, and there is wide variation in the protocols used by providers to communicate accounting information within their own organizations. Therefore, a roaming standard MUST prescribe a standardized format for accounting records. For the sake of efficiency, the record format MUST be compact.

Extensibility
A standard accounting record format MUST be able to encode metrics commonly used to determine the user's bill. Since these metrics

change over time, the accounting record format MUST be extensible so as to be able to add future metrics as they come along. The record format MUST support both standard metrics as well as vendor-specific metrics.

5. References

[1] Aboba, B., Lu, J., Alsop, J., Ding, J. and W. Wang, "Review of Roaming Implementations", RFC 2194, September 1997.

[2] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.

[3] Rigney, C., "RADIUS Accounting", RFC 2139, April 1997.

[4] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[5] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

[6] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[7] Blunk, L. and J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

[8] Simpson, W., "PPP Challenge Handshake Authentication Protocol (CHAP)", RFC 1994, August 1996.

[9] Lloyd, B. and Simpson, W., "PPP Authentication Protocols", RFC 1334, October 1992.

[10] Simpson, W., "The Point-to-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

6. Security Considerations

This document, being a requirements document, does not have any security concerns. The security requirements on protocols to be evaluated using this document are mainly described in section 5.2.

7. Acknowledgements

Thanks to Pat Calhoun (pcalhoun@eng.sun.com), Butch Anton (butch@ipass.com) and John Vollbrecht (jrv@merit.edu) for many useful discussions of this problem space.

8. Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-936-6605
EMail: bernarda@microsoft.com

Glen Zorn
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: 425-703-1559
EMail: glennz@microsoft.com

9. Full Copyright Statement