Network Working Group   G. Mansfield
Request for Comments: 2605   Cyber Solutions Inc.
Obsoletes: 1567   S. Kille
Category: Standards Track   MessagingDirect Ltd.
                                                         June 1999

                    Directory Server Monitoring MIB

Status of this Memo

Copyright Notice

Abstract

   This memo defines a portion of the Management Information Base (MIB)
   for use with network management protocols in the Internet community.
   This memo obsoletes RFC 1567, "X.500 Directory Monitoring MIB". This
   memo extends that specification to a more generic MIB for monitoring
   one or more directory servers each of which may support multiple
   access protocols. The MIB defined in this memo will be used in
   conjunction with the NETWORK-SERVICES-MIB [19] for monitoring
   Directory Servers.

Table of Contents

1. The SNMP Network Management Framework

    The SNMP Network Management Framework presently consists of five
    major components:

    o   An overall architecture, described in RFC 2571 [1].

    o   Mechanisms for describing and naming objects and events for the
         purpose of management. The first version of this Structure of
         Management Information (SMI) is called SMIv1 and described in
         STD 16, RFC 1155 [2], STD 16, RFC 1212 [3] and RFC 1215 [4]. The
         second version, called SMIv2, is described in STD 58, RFC 2578
         [5], RFC 2579 [6] and RFC 2580 [7].

    o   Message protocols for transferring management information. The
         first version of the SNMP message protocol is called SNMPv1 and
         described in STD 15, RFC 1157 [8]. A second version of the SNMP
         message protocol, which is not an Internet standards track
         protocol, is called SNMPv2c and described in RFC 1901 [9] and
         RFC 1906 [10].   The third version of the message protocol is
         called SNMPv3 and described in RFC 1906 [10], RFC 2572 [11] and
         RFC 2574 [12].

    o   Protocol operations for accessing management information. The
         first set of protocol operations and associated PDU formats is
         described in STD 15, RFC 1157 [8]. A second set of protocol
         operations and associated PDU formats is described in RFC 1905
         [13].

    o   A set of fundamental applications described in RFC 2573 [14] and
         the view-based access control mechanism described in RFC 2575
         [15].

    Managed objects are accessed via a virtual information store, termed
    the Management Information Base or MIB. Objects in the MIB are
    defined using the mechanisms defined in the SMI.

    This memo specifies a MIB module that is compliant to the SMIv2. A
    MIB conforming to the SMIv1 can be produced through the appropriate
    translations. The resulting translated MIB must be semantically
    equivalent, except where objects or events are omitted because no
    translation is possible (use of Counter64). Some machine readable
    information in SMIv2 will be converted into textual descriptions in
    SMIv1 during the translation process. However, this loss of machine
    readable information is not considered to change the semantics of the
    MIB.

2. The Directory Services Model.

   The Directory comprises of a set of servers (Directory Servers).
   Clients or Directory User Agents (DUA) are provided access to the
   Directory which maybe local or distributed, by the Directory Servers.
   The server maybe a X.500 Directory System Agent (DSA) [16] running
   over the OSI suite of protocols or, a (C)LDAP[17,18] frontend to the
   X.500 Directory System Agent or, a native LDAP Directory Server
   running directly over TCP or other protocols, or a database acting as
   a backend to another server, or any other application protocol, or
   any combination of the above. A Directory Server has one or more
   application protocol interfaces. Through these interfaces the
   Directory Server interacts with the DUA and with the peer Directory
   Servers.

   Fig. 1 shows the case of a Directory Server that receives requests
   and sends back responses in some protocol. Fig. 2 shows one possible
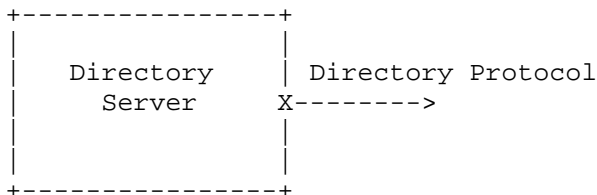   scenario where the Directory Server speaks multiple protocols.

```
                     +----------------+
                     |                |
                     |   Directory    | Directory Protocol
                     |    Server      X-------->
                     |                |
                     |                |
                     +----------------+

                          FIG. 1.


                     +----------------+
                     |                |
            DSP <----------X                X--------> DAP
                     |   Directory    |
          Other      |    Server      |
        Protocol <----------X                X--------> LDAP
                     |                |
                     +----------------+

                          FIG. 2.
```
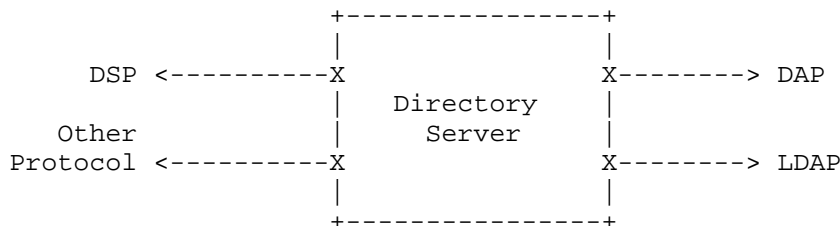
   The Directory contains information in the form of entries. An entry
   is a collection of attributes and is uniquely identified by a name,
   the Distinguished Name (DN). The entries are arranged in a
   hierarchical tree-like structure called the Directory Information
   Tree (DIT).

A DUA requests a Directory Server to perform some operation on the
Directory. The Directory Server is responsible for performing the
operation and after completing its effort to carry out the request,
returns a response to the DUA.

A Directory Server may use information stored in its local database
or interact with (chain the request to) other Directory Servers to
service the DUA request. Alternatively, a Directory Server may return
a reference to another Directory Server (referral).

The local database of a Directory Server consists of the part of the
Directory that is mastered by the Directory Server, the part of the
Directory for which it keeps slave copies and cached information that
is gathered during the operation of the Directory Server.

In the connection oriented mode a DUA "binds" to a Directory Server
with a particular identification. The Directory Server may
authenticate the identity of the DUA. In the connectionless mode as
is employed in CLDAP no binding and/or authentication is carried out
between the DUA and the Directory Server. The following type of
operations are carried out by the Directory Server : Read, Compare,
Addition of an Entry (AddEntry), Modification of an Entry
(ModifyEntry), Modification of a DN (ModifyRDN), Deletion of an Entry
(RemoveEntry), List, Search, Abandon. Some Directory Servers do not
support some type of operations. For example CLDAP does not support
AddEntry, ModifyEntry, ModifyRDN, RemoveEntry etc. In response to
requests results and/or errors are returned by the Directory Server.

In the distributed Directory data is often replicated to enhance
performance and for other advantages. The data to be replicated is
transferred from the "Supplier" Directory Server to the "Consumer"
Directory Server according to the replication agreement between the
supplier and the receiver.

3. MIB Model for Directory Management.

A Directory manager should be able to monitor all the Directory
Servers in his/her domain of management. The Directory Servers may be
running on one or more hosts and, multiple Directory Servers may be
running on the same host.

The manager may wish to monitor several aspects of the operational
Directory Servers. He/she may want to know the process related
aspects - the resource utilization of an operational Directory
Server; the network service related aspects e.g. inbound-
associations, outbound-associations, operational status, and finally
the information specific to the Directory Server application - its
operations and performance.

The MIB defined in this document covers the portion which is specific
to Directory services. The network service related part of the MIB,
and the host-resources related part of the MIB, as well as other
parts of interest to a Manager monitoring the Directory services, are
covered in separate documents [19] [20].

The MIB will cover a group of Directory Servers. The grouping will be
done on some logical basis by the administrator/manager. In all
cases, the grouping will be reflected in the pertinent NETWORK-
SERVICES-MIB which will have an entry corresponding to each Directory
Server in the group.

4. MIB design.

The basic principle has been to keep the MIB as simple as possible.
The Managed objects included in the MIB are divided into three tables
- dsTable, dsApplIfOpsTable, and dsIntTable.

   - The dsTable contains a list of Directory Servers. The list
     contains a description of the Directory Servers as well as
     summary statistics on the entries held by and the cache
     performance of each Directory Server. The group of servers on
     this list is likely to contain a part of, if not all, the
     Directory Servers in the management domain.

   - The dsApplIfOpsTable provides summary statistics on the
     accesses, operations and errors for each application protocol
     interface of a Directory Server.

   - The dsIntTable provides some useful information on the
     interaction of the monitored Directory Servers with peer
     Directory Servers.

There are references to the Directory itself for static information
pertaining to the Directory Server. These references are in the form
of "Directory Distinguished Name" [21] of the corresponding object.
It is intended that Directory management applications will use these
references to obtain further information on the objects of interest.

5. The Directory Server Monitoring MIB.

    DIRECTORY-SERVER-MIB DEFINITIONS ::= BEGIN

     IMPORTS
       MODULE-IDENTITY, Counter32, Gauge32, OBJECT-TYPE
                 FROM SNMPv2-SMI
       mib-2   FROM RFC1213-MIB
       DisplayString,   TimeStamp

```
                FROM SNMPv2-TC
        MODULE-COMPLIANCE, OBJECT-GROUP
                FROM SNMPv2-CONF
        ZeroBasedCounter32
                FROM RMON2-MIB
        applIndex, DistinguishedName, URLString

                FROM NETWORK-SERVICES-MIB;


    dsMIB MODULE-IDENTITY
       LAST-UPDATED "9906070000Z"
       ORGANIZATION "IETF Mail and Directory Management Working
                     Group"
       CONTACT-INFO
       "                         Glenn Mansfield
                      Postal: Cyber Solutions Inc.
                              6-6-3, Minami Yoshinari
                              Aoba-ku, Sendai, Japan 989-3204.

                         Tel: +81-22-303-4012
                         Fax: +81-22-303-4015
                    E-mail: glenn@cysols.com
        Working Group E-mail: ietf-madman@innosoft.com
              To subscribe: ietf-madman-request@innosoft.com"

       DESCRIPTION
               " The MIB module for monitoring Directory Services."

       -- revision information


       REVISION "9906070000Z"
       DESCRIPTION
         "This revision of this MIB is published in RFC 2605.

          This revision obsoletes RFC 1567. It is incompatible with
          the original MIB and so it has been renamed from dsaMIB
          to dsMIB."

       REVISION "9311250000Z" -- 25th November 1993
       DESCRIPTION
         "The original version of this MIB was published in RFC 1567."
       ::= { mib-2 66 }

    dsTable OBJECT-TYPE
        SYNTAX SEQUENCE OF DsTableEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
```

```
            " The table holding information related to the Directory
              Servers."
          ::= {dsMIB 1}

     dsTableEntry OBJECT-TYPE
         SYNTAX DsTableEntry
         MAX-ACCESS not-accessible
         STATUS current
         DESCRIPTION
           " Entry containing summary description for a Directory
             Server."
         INDEX { applIndex }
         ::= {dsTable 1}

   -- General description of the Directory Server application will be
   -- available in the applTable of the NETWORK-SERVICES-MIB indexed by
   -- applIndex.

    DsTableEntry ::= SEQUENCE {
        dsServerType
            BITS,
        dsServerDescription
            DisplayString,

    -- Entry statistics/Cache performance
        dsMasterEntries
            Gauge32,
        dsCopyEntries
            Gauge32,
        dsCacheEntries
            Gauge32,
        dsCacheHits
            Counter32,
        dsSlaveHits
            Counter32
    }

    dsServerType OBJECT-TYPE
        SYNTAX BITS {
                    frontEndDirectoryServer(0),
                    backEndDirectoryServer(1)
               }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "This object indicates whether the server is
           a frontend or, a backend or, both. If the server
           is a frontend, then the frontEndDirectoryServer
```

```
           bit will be set. Similarly for the backend."
        ::= {dsTableEntry 1}

   dsServerDescription OBJECT-TYPE
      SYNTAX DisplayString
      MAX-ACCESS read-only
      STATUS current
      DESCRIPTION
        "A text description of the application.  This information
         is intended to identify and briefly describe the
         application in a status display."
        ::= {dsTableEntry 2}


  -- A (C)LDAP frontend to the X.500 Directory will not have
  -- MasterEntries, CopyEntries; the following counters will
  -- be inaccessible for LDAP/CLDAP frontends to the X.500
  -- directory: dsMasterEntries, dsCopyEntries, dsSlaveHits.

   dsMasterEntries OBJECT-TYPE
       SYNTAX Gauge32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         " Number of entries mastered in the Directory Server."
       ::= {dsTableEntry 3}

   dsCopyEntries OBJECT-TYPE
       SYNTAX Gauge32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         " Number of entries for which systematic (slave)
           copies are maintained in the Directory Server."
       ::= {dsTableEntry 4}

   dsCacheEntries OBJECT-TYPE
       SYNTAX Gauge32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         " Number of entries cached (non-systematic copies) in
           the Directory Server. This will include the entries that
           are cached partially. The negative cache is not counted."
       ::= {dsTableEntry 5}

   dsCacheHits OBJECT-TYPE
       SYNTAX Counter32
```

```
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of operations that were serviced from
            the locally held cache."
        ::= {dsTableEntry 6}

    dsSlaveHits  OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of operations that were serviced from
            the locally held object replications ( copy-
            entries)."
        ::= {dsTableEntry 7}

    dsApplIfOpsTable OBJECT-TYPE
        SYNTAX SEQUENCE OF DsApplIfOpsEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
          " The table holding information related to the
            Directory Server operations."
        ::= {dsMIB 2}

    dsApplIfOpsEntry OBJECT-TYPE
        SYNTAX DsApplIfOpsEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
          " Entry containing operations related statistics
            for a Directory Server."
        INDEX { applIndex, dsApplIfProtocolIndex }
        ::= {dsApplIfOpsTable 1}
    DsApplIfOpsEntry ::= SEQUENCE {

        dsApplIfProtocolIndex
             INTEGER,
        dsApplIfProtocol
             OBJECT IDENTIFIER,

    -- Bindings

        dsApplIfUnauthBinds
            Counter32,
        dsApplIfSimpleAuthBinds
            Counter32,
```

```
         dsApplIfStrongAuthBinds
             Counter32,
         dsApplIfBindSecurityErrors
             Counter32,

     -- In-coming operations

         dsApplIfInOps
             Counter32,
         dsApplIfReadOps
             Counter32,
         dsApplIfCompareOps
             Counter32,
         dsApplIfAddEntryOps
             Counter32,
         dsApplIfRemoveEntryOps
             Counter32,
         dsApplIfModifyEntryOps
             Counter32,
         dsApplIfModifyRDNOps
             Counter32,
         dsApplIfListOps
             Counter32,
         dsApplIfSearchOps
             Counter32,
         dsApplIfOneLevelSearchOps
             Counter32,
         dsApplIfWholeSubtreeSearchOps
             Counter32,

     -- Out going operations

         dsApplIfReferrals
             Counter32,
         dsApplIfChainings
             Counter32,

     -- Errors

         dsApplIfSecurityErrors
             Counter32,
         dsApplIfErrors
             Counter32,

     -- replications

         dsApplIfReplicationUpdatesIn
             Counter32,
```

```
       dsApplIfReplicationUpdatesOut
           Counter32,

   -- Traffic Volume

       dsApplIfInBytes
           Counter32,
       dsApplIfOutBytes
           Counter32
   }

-- CLDAP does not use binds; for the CLDAP interface of a Directory
-- Server the bind related counters will be inaccessible.
--
-- CLDAP and LDAP implement "Read" and "List" operations
-- indirectly via the "search" operation; the following
-- counters will be inaccessible for the CLDAP and LDAP interfaces of
-- Directory Servers:  dsApplIfReadOps, dsApplIfListOps
--
-- CLDAP does not implement "Compare", "Add", "Remove",
-- "Modify", "ModifyRDN"; the following counters will be
-- inaccessible for the CLDAP interfaces of Directory Servers:
-- dsApplIfCompareOps, dsApplIfAddEntryOps,  dsApplIfRemoveEntryOps,
-- dsApplIfModifyEntryOps, dsApplIfModifyRDNOps.
--
-- CLDAP Directory Servers do not return Referrals
-- the following fields will remain inaccessible for
-- CLDAP interfaces of Directory Servers: dsApplIfReferrals.

   dsApplIfProtocolIndex OBJECT-TYPE
       SYNTAX INTEGER (1..2147483647)
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
        "An index to uniquely identify an entry corresponding to a
         application-layer protocol interface. This index is used
         for lexicographic ordering of the table."
       ::= {dsApplIfOpsEntry 1}

   dsApplIfProtocol OBJECT-TYPE
       SYNTAX OBJECT IDENTIFIER
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
        "An identification of the protocol being used by the application
         on this interface.  For an OSI Application, this will be the
         Application Context.  For Internet applications, the IANA
         maintains a registry[22] of the OIDs which correspond to
```

          well-known applications. If the application protocol is
          not listed in the registry, an OID value of the form
          {applTCPProtoID port} or {applUDProtoID port} are used for
          TCP-based and UDP-based protocols, respectively. In either
          case 'port' corresponds to the primary port number being
          used by the protocol. The OIDs applTCPProtoID and
          applUDPProtoID are defined in NETWORK-SERVICES-MIB"
        ::= {dsApplIfOpsEntry 2}

    dsApplIfUnauthBinds OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of unauthenticated/anonymous bind requests
            received."
        ::= {dsApplIfOpsEntry 3}

    dsApplIfSimpleAuthBinds OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of bind requests that were authenticated
            using simple authentication procedures like password
            checks. This includes the
            password authentication using SASL mechanisms like
            CRAM-MD5."
        ::= {dsApplIfOpsEntry 4}

    dsApplIfStrongAuthBinds OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of bind requests that were authenticated
            using TLS and X.500 strong authentication procedures.
            This includes the binds that were
            authenticated using external authentication procedures."
        ::= {dsApplIfOpsEntry 5}

    dsApplIfBindSecurityErrors OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of bind requests that have been rejected
            due to inappropriate authentication or

              invalid credentials."
          ::= {dsApplIfOpsEntry 6}

      dsApplIfInOps OBJECT-TYPE
          SYNTAX Counter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Number of requests received from DUAs or other
              Directory Servers."
          ::= {dsApplIfOpsEntry 7}

      dsApplIfReadOps OBJECT-TYPE
          SYNTAX Counter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Number of read requests received."
          ::= {dsApplIfOpsEntry 8}

      dsApplIfCompareOps OBJECT-TYPE
          SYNTAX Counter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Number of compare requests received."
          ::= {dsApplIfOpsEntry 9}

      dsApplIfAddEntryOps OBJECT-TYPE
          SYNTAX Counter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Number of addEntry requests received."
          ::= {dsApplIfOpsEntry 10}

      dsApplIfRemoveEntryOps OBJECT-TYPE
          SYNTAX Counter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Number of removeEntry requests received."
          ::= {dsApplIfOpsEntry 11}

      dsApplIfModifyEntryOps OBJECT-TYPE

```
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of modifyEntry requests received."
        ::= {dsApplIfOpsEntry 12}


    dsApplIfModifyRDNOps OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of modifyRDN requests received."
        ::= {dsApplIfOpsEntry 13}

    dsApplIfListOps OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of list requests received."
        ::= {dsApplIfOpsEntry 14}

    dsApplIfSearchOps OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of search requests- baseObject searches,
            oneLevel searches and  whole subtree searches,
            received."
        ::= {dsApplIfOpsEntry 15}

    dsApplIfOneLevelSearchOps OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          " Number of oneLevel search requests received."
        ::= {dsApplIfOpsEntry 16}


    dsApplIfWholeSubtreeSearchOps   OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
```

```
                " Number of whole subtree search requests received."
             ::= {dsApplIfOpsEntry 17}


        dsApplIfReferrals OBJECT-TYPE
            SYNTAX Counter32
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
              " Number of referrals returned in response
                to requests for operations."
             ::= {dsApplIfOpsEntry 18}

        dsApplIfChainings OBJECT-TYPE
            SYNTAX Counter32
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
              " Number of operations forwarded by this Directory Server
                to other Directory Servers."
             ::= {dsApplIfOpsEntry 19}

        dsApplIfSecurityErrors OBJECT-TYPE
            SYNTAX Counter32
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
              " Number of requests received
                which did not meet the security requirements. "
             ::= {dsApplIfOpsEntry 20}

        dsApplIfErrors  OBJECT-TYPE
            SYNTAX Counter32
            MAX-ACCESS read-only
            STATUS current
            DESCRIPTION
              " Number of requests that could not be serviced
                due to errors other than security errors, and
                referrals.
                A partially serviced operation will not be counted
                as an error.
                The errors include naming-related, update-related,
                attribute-related and service-related errors."
             ::= {dsApplIfOpsEntry 21}

      -- Replication operations

       dsApplIfReplicationUpdatesIn OBJECT-TYPE
```

```
     SYNTAX Counter32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " Number of replication updates fetched or received from
         supplier Directory Servers."
     ::= {dsApplIfOpsEntry 22}


dsApplIfReplicationUpdatesOut OBJECT-TYPE
     SYNTAX Counter32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " Number of replication updates sent to or taken by
         consumer Directory Servers."
     ::= {dsApplIfOpsEntry 23}


dsApplIfInBytes  OBJECT-TYPE
     SYNTAX Counter32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " Incoming traffic, in bytes, on the interface.
         This will include requests from DUAs as well
         as responses from other Directory Servers."
     ::= {dsApplIfOpsEntry 24}


dsApplIfOutBytes OBJECT-TYPE
     SYNTAX Counter32
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " Outgoing traffic in bytes on the interface.
         This will include responses to DUAs and Directory
         Servers as well as requests to other Directory Servers."
     ::= {dsApplIfOpsEntry 25}



-- The dsIntTable contains statistical data on the peer
-- Directory Servers  with which the monitored Directory
-- Server interacts or, attempts to interact. This  table is
-- expected to provide a useful insight into the effect of
-- neighbours on the Directory Server's performance.
-- The table keeps track of the last "N" Directory Servers
-- with which  the  monitored  Directory  has  interacted
-- (attempted to interact), where "N" is a locally-defined
-- constant.
-- For a multiprotocol server, statistics for each protocol
```

```
     -- are kept separetely.

     dsIntTable OBJECT-TYPE
         SYNTAX   SEQUENCE OF DsIntEntry
         MAX-ACCESS  not-accessible
         STATUS  current
         DESCRIPTION
           " Each row of this table contains some details
             related to the history of the interaction
             of the monitored Directory Server with its
             peer Directory Servers."
         ::= { dsMIB 3 }

     dsIntEntry OBJECT-TYPE
         SYNTAX   DsIntEntry
         MAX-ACCESS  not-accessible
         STATUS   current
         DESCRIPTION
           " Entry containing interaction details of a Directory
             Server with a peer Directory Server."
         INDEX { applIndex,dsIntEntIndex, dsApplIfProtocolIndex }
         ::= { dsIntTable 1 }

     DsIntEntry ::= SEQUENCE {
        dsIntEntIndex
                  INTEGER,
        dsIntEntDirectoryName
                  DistinguishedName,
        dsIntEntTimeOfCreation
                  TimeStamp,
        dsIntEntTimeOfLastAttempt
                  TimeStamp,
        dsIntEntTimeOfLastSuccess
                  TimeStamp,
        dsIntEntFailuresSinceLastSuccess
                  Gauge32,
        dsIntEntFailures
                  ZeroBasedCounter32,
        dsIntEntSuccesses
                  ZeroBasedCounter32,
        dsIntEntURL
                  URLString
     }

     dsIntEntIndex  OBJECT-TYPE
         SYNTAX INTEGER (1..2147483647)
         MAX-ACCESS not-accessible
         STATUS current
```

```
     DESCRIPTION
       " Together with applIndex and dsApplIfProtocolIndex, this
         object forms the unique key to
         identify the conceptual row which contains useful info
         on the (attempted) interaction between the Directory
         Server (referred to by applIndex) and a peer Directory
         Server using a particular protocol."
     ::= {dsIntEntry 1}

 dsIntEntDirectoryName   OBJECT-TYPE
     SYNTAX DistinguishedName
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " Distinguished Name of the peer Directory Server to
         which this entry pertains."
     ::= {dsIntEntry 2}

 dsIntEntTimeOfCreation   OBJECT-TYPE
     SYNTAX TimeStamp
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " The value of sysUpTime when this row was created.
         If the entry was created before the network management
         subsystem was initialized, this object will contain
         a value of zero."
     ::= {dsIntEntry 3}

 dsIntEntTimeOfLastAttempt   OBJECT-TYPE
     SYNTAX TimeStamp
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " The value of sysUpTime when the last attempt was made
         to contact the peer Directory Server. If the last attempt
         was made before the network management subsystem was
         initialized, this object will contain a value of zero."
     ::= {dsIntEntry 4}

 dsIntEntTimeOfLastSuccess   OBJECT-TYPE
     SYNTAX TimeStamp
     MAX-ACCESS read-only
     STATUS current
     DESCRIPTION
       " The value of sysUpTime when the last attempt made to
         contact the peer Directory Server was successful. If there
         have been no successful attempts this entry will have a value
```

             of zero. If the last successful attempt was made before
             the network management subsystem was initialized, this
             object will contain a value of zero."
          ::= {dsIntEntry 5}

      dsIntEntFailuresSinceLastSuccess OBJECT-TYPE
          SYNTAX Gauge32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " The number of failures since the last time an
              attempt to contact the peer Directory Server was successful.
              If there have been no successful attempts, this counter
              will contain the number of failures since this entry
              was created."
          ::= {dsIntEntry 6}

    -- note this gauge has a maximum value of 4294967295 and,
    -- it does not wrap.[5]

     dsIntEntFailures OBJECT-TYPE
          SYNTAX ZeroBasedCounter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Cumulative failures in contacting the peer Directory Server
              since the creation of this entry."
          ::= {dsIntEntry 7}

     dsIntEntSuccesses OBJECT-TYPE
          SYNTAX ZeroBasedCounter32
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " Cumulative successes in contacting the peer Directory Server
              since the creation of this entry."
          ::= {dsIntEntry 8}

     dsIntEntURL OBJECT-TYPE
          SYNTAX URLString
          MAX-ACCESS read-only
          STATUS current
          DESCRIPTION
            " URL of the peer Directory Server."
          ::= {dsIntEntry 9}

     -- Conformance information

     dsConformance OBJECT IDENTIFIER ::= { dsMIB 4 }

     dsGroups   OBJECT IDENTIFIER ::= { dsConformance 1 }
     dsCompliances OBJECT IDENTIFIER ::= { dsConformance 2 }

     -- Compliance statements

     dsEntryCompliance MODULE-COMPLIANCE
         STATUS current
         DESCRIPTION
                 "The compliance statement for SNMP entities
                 which implement the DIRECTORY-SERVER-MIB for
                 a summary overview of the Directory Servers ."

         MODULE -- this module
            MANDATORY-GROUPS { dsEntryGroup }

         ::= { dsCompliances 1 }

     dsOpsCompliance MODULE-COMPLIANCE
         STATUS current
         DESCRIPTION
                 "The compliance statement for SNMP entities
                 which implement the DIRECTORY-SERVER-MIB for monitoring
                 Directory Server operations, entry statistics and cache
                 performance."

         MODULE -- this module
            MANDATORY-GROUPS { dsEntryGroup, dsOpsGroup }

         ::= { dsCompliances 2 }

     dsIntCompliance MODULE-COMPLIANCE
           STATUS current
           DESCRIPTION
                   " The compliance statement for SNMP entities
                    which implement the DIRECTORY-SERVER-MIB for
                    monitoring Directory Server operations and the
                    interaction of the Directory Server with peer
                    Directory Servers."

           MODULE -- this module
           MANDATORY-GROUPS { dsEntryGroup, dsIntGroup }

           ::= { dsCompliances 3 }

     dsOpsIntCompliance MODULE-COMPLIANCE
         STATUS current

            DESCRIPTION
                    " The compliance statement for SNMP   entities
                      which implement the DIRECTORY-SERVER-MIB for monitoring
                      Directory Server operations and the interaction of the
                      Directory Server with peer Directory Servers."

            MODULE -- this module
            MANDATORY-GROUPS { dsEntryGroup, dsOpsGroup, dsIntGroup }

            ::= { dsCompliances 4 }

    -- Units of conformance

    dsEntryGroup   OBJECT-GROUP
        OBJECTS {dsServerType,   dsServerDescription,
                 dsMasterEntries,   dsCopyEntries,
                 dsCacheEntries,   dsCacheHits,
                 dsSlaveHits}
        STATUS current
        DESCRIPTION
                " A collection of objects for a summary overview of the
                  Directory Servers."
        ::= { dsGroups 1 }

    dsOpsGroup   OBJECT-GROUP
        OBJECTS {
          dsApplIfProtocolIndex,   dsApplIfProtocol,
          dsApplIfUnauthBinds,   dsApplIfSimpleAuthBinds,
          dsApplIfStrongAuthBinds,   dsApplIfBindSecurityErrors,
          dsApplIfInOps,   dsApplIfReadOps,
          dsApplIfCompareOps,   dsApplIfAddEntryOps,
          dsApplIfRemoveEntryOps,   dsApplIfModifyEntryOps,
          dsApplIfModifyRDNOps,   dsApplIfListOps,
          dsApplIfSearchOps,   dsApplIfOneLevelSearchOps,
          dsApplIfWholeSubtreeSearchOps, dsApplIfReferrals,
          dsApplIfChainings,   dsApplIfSecurityErrors,
          dsApplIfErrors,   dsApplIfReplicationUpdatesIn,
          dsApplIfReplicationUpdatesOut, dsApplIfInBytes,
          dsApplIfOutBytes   }
        STATUS current
        DESCRIPTION
                " A collection of objects for monitoring the Directory
                  Server operations."
        ::= { dsGroups 2 }

    dsIntGroup   OBJECT-GROUP
        OBJECTS {

```
        dsIntEntDirectoryName,         dsIntEntTimeOfCreation,
        dsIntEntTimeOfLastAttempt,     dsIntEntTimeOfLastSuccess,
        dsIntEntFailuresSinceLastSuccess, dsIntEntFailures,
        dsIntEntSuccesses,             dsIntEntURL}
    STATUS  current
    DESCRIPTION
            " A collection of objects for monitoring the Directory
              Server's interaction with peer Directory Servers."
    ::= { dsGroups 3 }


    END
```

6. Intellectual Property

   The IETF takes no position regarding the validity or scope of any
   intellectual property or other rights that might be claimed to
   pertain to the implementation or use of the technology described in
   this document or the extent to which any license under such rights
   might or might not be available; neither does it represent that it
   has made any effort to identify any such rights. Information on the
   IETF's procedures with respect to rights in standards-track and
   standards-related documentation can be found in BCP-11. Copies of
   claims of rights made available for publication and any assurances of
   licenses to be made available, or the result of an attempt made to
   obtain a general license or permission for the use of such
   proprietary rights by implementors or users of this specification can
   be obtained from the IETF Secretariat.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights which may cover technology that may be required to practice
   this standard. Please address the information to the IETF Executive
   Director.

7. Changes from RFC1567.

   A more general Directory model in which, several Directory protocols
   coexist, has been adopted for the purpose of the MIB design. The
   result is a generic Directory Server Monitoring MIB.

8. Acknowledgements

   This memo is the product of discussions and deliberations carried out
   in the Mail and Directory Management Working Group (ietf-madman-wg).

References

   [1]   Harrington, D., Presuhn, R. and B. Wijnen, "An Architecture for
         Describing SNMP Management Frameworks", RFC 2571, April 1999.

   [2]   Rose, M. and K. McCloghrie, "Structure and Identification of
         Management Information for TCP/IP-based Internets", STD 16, RFC
         1155, May 1990.

   [3]   Rose, M. and K. McCloghrie, "Concise MIB Definitions", STD 16,
         RFC 1212, March 1991.

   [4]   Rose, M., "A Convention for Defining Traps for use with the
         SNMP", RFC 1215, March 1991.

   [5]   McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose,
         M. and S. Waldbusser, "Structure of Management Information
         Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

   [6]   McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose,
         M. and S. Waldbusser, "Textual Conventions for SMIv2", STD 58,
         RFC 2579, April 1999.

   [7]   McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose,
         M. and S. Waldbusser, "Conformance Statements for SMIv2", STD
         58, RFC 2580, April 1999.

   [8]   Case, J., Fedor, M., Schoffstall, M. and J. Davin, "Simple
         Network Management Protocol", STD 15, RFC 1157, May 1990.

   [9]   Case, J., McCloghrie, K., Rose, M. and S. Waldbusser,
         "Introduction to Community-based SNMPv2", RFC 1901, January
         1996.

   [10] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Transport
         Mappings for Version 2 of the Simple Network Management Protocol
         (SNMPv2)", RFC 1906, January 1996.

   [11] Case, J., Harrington D., Presuhn R. and B. Wijnen, "Message
         Processing and Dispatching for the Simple Network Management
         Protocol (SNMP)", RFC 2572, April 1999.

   [12] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM)
         for version 3 of the Simple Network Management Protocol
         (SNMPv3)", RFC 2574, April 1999.

   [13] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Protocol
        Operations for Version 2 of the Simple Network Management
        Protocol (SNMPv2)", RFC 1905, January 1996.

   [14] Levi, D., Meyer, P. and B. Stewart, "SNMPv3 Applications", RFC
        2573, April 1999.

   [15] Wijnen, B., Presuhn, R. and K. McCloghrie, "View-based Access
        Control Model (VACM) for the Simple Network Management Protocol
        (SNMP)", RFC 2575, April 1999.

   [16] ITU-T Rec. X.501, "The Directory: Models", 1993.

   [17] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access
        Protocol (v3)", RFC 2251, December 1997.

   [18] Young, A., "Connection-less Lightweight X.500 Directory Access
        Protocol", RFC 1798, June 1995.

   [19] Freed N. and Kille, S., "Network Services Monitoring MIB", RFC
        2248, January 1998.

   [20] Grillo, P. and S. Waldbusser, "Host Resources MIB", RFC 1514,
        September 1993.

   [21] Wahl, W., Kille, S. and T. Howes, "Lightweight Directory Access
        Protocol (v3): UTF-8 String Representation of Distinguished
        Names", RFC 2253, December 1997.

   [22] http://www.isi.edu/in-notes/iana/assignments/protocol-numbers

Security Considerations

   There are no management objects defined in this MIB that have a MAX-
   ACCESS clause of read-write and/or read-create. So, if this MIB is
   implemented correctly, then there is no risk that an intruder can
   alter or create any management objects of this MIB via direct SNMP
   SET operations.

   However, the information itself may partly reveal the configuration
   of the directory system and passively increase its vulnerability. The
   information could also be used to analyze network usage and traffic
   patterns.

   Therefore, it may be important in some environments to control read
   access to these objects and possibly to even encrypt the values of
   these object when sending them over the network via SNMP. Not all
   versions of SNMP provide features for such a secure environment.

SNMPv1 by itself is such an insecure environment. Even if the
network itself is secure (for example by using IPSec), even then,
there is no control as to who on the secure network is allowed to
access and GET (read) the objects in this MIB.

It is recommended that the implementors consider the security
features as provided by the SNMPv3 framework. Specifically, the use
of the User-based Security Model RFC 2574 [12] and the View-based
Access Control Model RFC 2575 [15] is recommended.

It is then a customer/user responsibility to ensure that the SNMP
entity giving access to an instance of this MIB, is properly
configured to give access to those objects only to those principals
(users) that have legitimate rights to access them.

Authors' Addresses

    Glenn Mansfield
    Cyber Solutions Inc.
    6-6-3 Minami Yoshinari
    Aoba-ku, Sendai 989-3204
    Japan

    Phone: +81-22-303-4012
    EMail: glenn@cysols.com

    Steve E. Kille
    MessagingDirect Ltd.
    The Dome, The Square
    Richmond TW9 1DT
    UK

    Phone: +44-181-332-9091
    EMail: Steve.Kille@MessagingDirect.com

Full Copyright Statement

Acknowledgement