                     Network Services Monitoring MIB

Status of this Memo

Copyright Notice

Introduction

   A networked application is a realization of some well-defined service
   on one or more host computers that is accessible via some network,
   uses some network for its internal operations, or both.

   There are a wide range of networked applications for which it is
   appropriate to provide SNMP monitoring of their network usage. This
   includes applications using both TCP/IP and OSI networking. This
   document defines a MIB which contains the elements common to the
   monitoring of any network service application. This information
   includes a table of all monitorable network service applications, a
   count of the associations (connections) to each application, and
   basic information about the parameters and status of each
   application-related association.

   This MIB may be used on its own for any application, and for most
   simple applications this will suffice. This MIB is also designed to
   serve as a building block which can be used in conjunction with
   application-specific monitoring and management. Two examples of this
   are MIBs defining additional variables for monitoring a Message
   Transfer Agent (MTA) service or a Directory Service Agent (DSA)
   service. It is expected that further MIBs of this nature will be
   specified.

This MIB does not attempt to provide facilities for management of the
host or hosts the network service application runs on, nor does it
provide facilities for monitoring applications that provide something
other than a network service. Host resource and general application
monitoring is handled by either the Host Resources MIB [1] or the
application MIB [2].

Table of Contents

1. The SNMP Network Management Framework

    The SNMP Management Framework presently consists of five major
    components:

    o   An overall architecture, described in RFC 2571 [3].

    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 [4], STD 16, RFC 1212 [5] and RFC 1215 [6]. The
         second version, called SMIv2, is described in STD 58, RFC 2578
         [7], STD 58, RFC 2579 [8] and STD 58, RFC 2580 [9].

    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 [10]. A second version of the SNMP
         message protocol, which is not an Internet standards track
         protocol, is called SNMPv2c and described in RFC 1901 [11] and
         RFC 1906 [12]. The third version of the message protocol is
         called SNMPv3 and described in RFC 1906 [12], RFC 2572 [13] and
         RFC 2574 [14].

   o   Protocol operations for accessing management information. The
        first set of protocol operations and associated PDU formats is
        described in STD 15, RFC 1157 [10]. A second set of protocol
        operations and associated PDU formats is described in RFC 1905
        [15].

   o   A set of fundamental applications described in RFC 2573 [16] and
        the view-based access control mechanism described in RFC 2575
        [17].

   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. Rationale for having a Network Services Monitoring MIB

   Much effort has been expended in developing tools to manage lower
   layer network facilities. However, relatively little work has been
   done on managing application layer entities. It is neither efficient
   nor reasonable to manage all aspects of application layer entities
   using only lower layer information. Moreover, the difficulty of
   managing application entities in this way increases dramatically as
   application entities become more complex.

   This leads to a substantial need to monitor applications which
   provide network services, particularly distributed components such as
   MTAs and DSAs, by monitoring specific aspects of the application
   itself. Reasons to monitor such components include but are not
   limited to measuring load, detecting broken connectivity, isolating
   system failures, and locating congestion.

   In order to manage network service applications effectively two
   requirements must be met:

   (1) It must be possible to monitor a large number of components
       (typical for a large organization).

   (2) Application monitoring must be integrated into general network
       management.

   This specification defines simple read-only access; this is
   sufficient to determine up/down status and provide an indication of a
   broad class of operational problems.

2.1. General Relationship to Other MIBs

   This MIB is intended to only provide facilities common to the
   monitoring of any network service application. It does not provide
   all the facilities necessary to monitor any specific application.
   Each specific type of network service application is expected to have
   a MIB of its own that makes use of these common facilities.

2.2. Restriction of Scope

   The framework provided here is very minimal; there is a lot more that
   could be done. For example:

   (1) General network service application configuration monitoring and
       control.

   (2) Detailed examination and modification of individual entries in
       service-specific request queues.

   (3) Probing to determine the status of a specific request (e.g., the
       location of a mail message with a specific message-id).

   (4) Requesting that certain actions be performed (e.g., forcing an
       immediate connection and transfer of pending messages to some
       specific system).

   All these capabilities are both impressive and useful. However,
   these capabilities would require provisions for strict security
   checking. These capabilities would also mandate a much more complex
   design, with many characteristics likely to be fairly
   implementation-specific. As a result such facilities are likely to
   be both contentious and difficult to implement.

   This document religiously keeps things simple and focuses on the
   basic monitoring aspect of managing applications providing network
   services. The goal here is to provide a framework which is simple,
   useful, and widely implementable.

2.3. Configuration Information

   This MIB attempts to provide information about the operational
   aspects of an application. Further information about the actual
   configuration of a given application may be kept in other places; the
   applDirectoryName or applURL may be used to point to places where
   such information is kept.

3. Application Objects

   This MIB defines a set of general purpose attributes which would be
   appropriate for a range of applications that provide network
   services. Both OSI and non-OSI services can be accommodated.
   Additional tables defined in extensions to this MIB provide
   attributes specific to specific network services.

   A table is defined which will have one row for each operational
   network service application on the system. The only static
   information held on the application is its name. All other static
   information should be obtained from various directory services. The
   applDirectoryName is an external key, which allows an SNMP MIB entry
   to be cleanly related to the X.500 Directory. In SNMP terms, the
   applications are grouped in a table called applTable, which is
   indexed by an integer key applIndex.

   The type of the application will be determined by one or both of:

     (1)   Additional MIB variables specific to the applications.

     (2)   An association to the application of a specific protocol.

4. Definitions

   NETWORK-SERVICES-MIB DEFINITIONS ::= BEGIN

   IMPORTS
       OBJECT-TYPE, Counter32, Gauge32, MODULE-IDENTITY, mib-2
         FROM SNMPv2-SMI
       TimeStamp, TEXTUAL-CONVENTION
         FROM SNMPv2-TC
       MODULE-COMPLIANCE, OBJECT-GROUP
         FROM SNMPv2-CONF
       SnmpAdminString
          FROM SNMP-FRAMEWORK-MIB;

   application MODULE-IDENTITY
       LAST-UPDATED "200003030000Z"
       ORGANIZATION "IETF Mail and Directory Management Working Group"

```
        CONTACT-INFO
          "        Ned Freed

           Postal: Innosoft International, Inc.
                   1050 Lakes Drive
                   West Covina, CA 91790
                   US

              Tel: +1 626 919 3600
              Fax: +1 626 919 3614

           E-Mail: ned.freed@innosoft.com"
        DESCRIPTION
          "The MIB module describing network service applications"
        REVISION "200003030000Z"
        DESCRIPTION
          "This revision, published in RFC 2788, changes a number of
           DisplayStrings to SnmpAdminStrings. Note that this change
           is not strictly supported by SMIv2.  However, the alternative
           of deprecating the old objects and defining new objects
           would have a more adverse impact on backward compatibility
           and interoperability, given the particular semantics of
           these objects. The defining reference for distinguished
           names has also been updated from RFC 1779 to RFC 2253."
        REVISION "199905120000Z"
        DESCRIPTION
          "This revision fixes a few small technical problems found
           in previous versions, mostly in regards to the conformance
           groups for different versions of this MIB.  No changes have
           been made to the objects this MIB defines since RFC 2248."
        REVISION "199708170000Z"
        DESCRIPTION
          "This revision, published in RFC 2248, adds the
           applDescription and applURL objects, adds the quiescing
           state to the applOperStatus object and renames the MIB
           from the APPLICATION-MIB to the NETWORK-SERVICE-MIB."
        REVISION "199311280000Z"
        DESCRIPTION
          "The original version of this MIB was published in RFC 1565"
        ::= {mib-2 27}

   -- Textual conventions

   -- DistinguishedName is used to refer to objects in the
   -- directory.

   DistinguishedName ::= TEXTUAL-CONVENTION
       DISPLAY-HINT "255a"
```

          STATUS current
          DESCRIPTION
              "A Distinguished Name represented in accordance with
               RFC 2253, presented in the UTF-8 charset defined in
               RFC 2279."
          SYNTAX OCTET STRING (SIZE (0..255))

    -- Uniform Resource Locators are stored in URLStrings.

    URLString ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "255a"
        STATUS current
        DESCRIPTION
            "A Uniform Resource Locator represented in accordance
             with RFCs 1738 and 2368, presented in the NVT ASCII
             charset defined in RFC 854."
        SYNTAX OCTET STRING (SIZE (0..255))

    -- The basic applTable contains a list of the application
    -- entities.

    applTable OBJECT-TYPE
        SYNTAX SEQUENCE OF ApplEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
            "The table holding objects which apply to all different
             kinds of applications providing network services.
             Each network service application capable of being
             monitored should have a single entry in this table."
        ::= {application 1}

    applEntry OBJECT-TYPE
        SYNTAX ApplEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
          "An entry associated with a single network service
           application."
        INDEX {applIndex}
        ::= {applTable 1}

    ApplEntry ::= SEQUENCE {
        applIndex
            INTEGER,
        applName
            SnmpAdminString,
        applDirectoryName

```
                DistinguishedName,
            applVersion
                SnmpAdminString,
            applUptime
                TimeStamp,
            applOperStatus
                INTEGER,
            applLastChange
                TimeStamp,
            applInboundAssociations
                Gauge32,
            applOutboundAssociations
                Gauge32,
            applAccumulatedInboundAssociations
                Counter32,
            applAccumulatedOutboundAssociations
                Counter32,
            applLastInboundActivity
                TimeStamp,
            applLastOutboundActivity
                TimeStamp,
            applRejectedInboundAssociations
                Counter32,
            applFailedOutboundAssociations
                Counter32,
            applDescription
                SnmpAdminString,
            applURL
                URLString
        }

    applIndex OBJECT-TYPE
        SYNTAX INTEGER (1..2147483647)
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
          "An index to uniquely identify the network service
           application. This attribute is the index used for
           lexicographic ordering of the table."
        ::= {applEntry 1}

    applName OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The name the network service application chooses to be
           known by."
```

```
        ::= {applEntry 2}

    applDirectoryName OBJECT-TYPE
        SYNTAX DistinguishedName
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The Distinguished Name of the directory entry where
           static information about this application is stored.
           An empty string indicates that no information about
           the application is available in the directory."
        ::= {applEntry 3}

    applVersion OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The version of network service application software.
           This field is usually defined by the vendor of the
           network service application software."
        ::= {applEntry 4}
    applUptime OBJECT-TYPE
        SYNTAX TimeStamp
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The value of sysUpTime at the time the network service
           application was last initialized.  If the application was
           last initialized prior to the last initialization of the
           network management subsystem, then this object contains
           a zero value."
        ::= {applEntry 5}

    applOperStatus OBJECT-TYPE
        SYNTAX INTEGER {
          up(1),
          down(2),
          halted(3),
          congested(4),
          restarting(5),
          quiescing(6)
        }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "Indicates the operational status of the network service
           application. 'down' indicates that the network service is
```

          not available. 'up' indicates that the network service
          is operational and available. 'halted' indicates that the
          service is operational but not available. 'congested'
          indicates that the service is operational but no additional
          inbound associations can be accommodated. 'restarting'
          indicates that the service is currently unavailable but is
          in the process of restarting and will be available soon.
          'quiescing' indicates that service is currently operational
          but is in the process of shutting down. Additional inbound
          associations may be rejected by applications in the
          'quiescing' state."
        ::= {applEntry 6}

   applLastChange OBJECT-TYPE
       SYNTAX TimeStamp
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "The value of sysUpTime at the time the network service
          application entered its current operational state. If
          the current state was entered prior to the last
          initialization of the local network management subsystem,
          then this object contains a zero value."
       ::= {applEntry 7}

   applInboundAssociations OBJECT-TYPE
       SYNTAX Gauge32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "The number of current associations to the network service
          application, where it is the responder. An inbound
          association occurs when another application successfully
          connects to this one."
       ::= {applEntry 8}

   applOutboundAssociations OBJECT-TYPE
       SYNTAX Gauge32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "The number of current associations to the network service
          application, where it is the initiator. An outbound
          association occurs when this application successfully
          connects to another one."
       ::= {applEntry 9}

   applAccumulatedInboundAssociations OBJECT-TYPE

        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The total number of associations to the application entity
           since application initialization, where it was the responder."
        ::= {applEntry 10}

    applAccumulatedOutboundAssociations OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The total number of associations to the application entity
           since application initialization, where it was the initiator."
        ::= {applEntry 11}

    applLastInboundActivity OBJECT-TYPE
        SYNTAX TimeStamp
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The value of sysUpTime at the time this application last
           had an inbound association. If the last association
           occurred prior to the last initialization of the network
           subsystem, then this object contains a zero value."
        ::= {applEntry 12}

    applLastOutboundActivity OBJECT-TYPE
        SYNTAX TimeStamp
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The value of sysUpTime at the time this application last
           had an outbound association. If the last association
           occurred prior to the last initialization of the network
           subsystem, then this object contains a zero value."
        ::= {applEntry 13}

    applRejectedInboundAssociations OBJECT-TYPE
        SYNTAX Counter32
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The total number of inbound associations the application
           entity has rejected, since application initialization.
           Rejected associations are not counted in the accumulated
           association totals. Note that this only counts

          associations the application entity has rejected itself;
          it does not count rejections that occur at lower layers
          of the network. Thus, this counter may not reflect the
          true number of failed inbound associations."
       ::= {applEntry 14}

   applFailedOutboundAssociations OBJECT-TYPE
       SYNTAX Counter32
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "The total number associations where the application entity
          is initiator and association establishment has failed,
          since application initialization. Failed associations are
          not counted in the accumulated association totals."
       ::= {applEntry 15}

   applDescription OBJECT-TYPE
       SYNTAX SnmpAdminString
       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."
       ::= {applEntry 16}

   applURL OBJECT-TYPE
       SYNTAX URLString
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "A URL pointing to a description of the application.
          This information is intended to identify and describe
          the application in a status display."
       ::= {applEntry 17}

   -- The assocTable augments the information in the applTable
   -- with information about associations. Note that two levels
   -- of compliance are specified below, depending on whether
   -- association monitoring is mandated.

   assocTable OBJECT-TYPE
       SYNTAX SEQUENCE OF AssocEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
           "The table holding a set of all active application

```
            associations."
      ::= {application 2}

   assocEntry OBJECT-TYPE
       SYNTAX AssocEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
         "An entry associated with an association for a network
          service application."
       INDEX {applIndex, assocIndex}
       ::= {assocTable 1}

   AssocEntry ::= SEQUENCE {
       assocIndex
           INTEGER,
       assocRemoteApplication
           SnmpAdminString,
       assocApplicationProtocol
           OBJECT IDENTIFIER,
       assocApplicationType
           INTEGER,
       assocDuration
           TimeStamp
   }

   assocIndex OBJECT-TYPE
       SYNTAX INTEGER (1..2147483647)
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
         "An index to uniquely identify each association for a network
          service application.  This attribute is the index that is
          used for lexicographic ordering of the table.  Note that the
          table is also indexed by the applIndex."
       ::= {assocEntry 1}

   assocRemoteApplication OBJECT-TYPE
       SYNTAX SnmpAdminString
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
         "The name of the system running remote network service
          application.  For an IP-based application this should be
          either a domain name or IP address.  For an OSI application
          it should be the string encoded distinguished name of the
          managed object.  For X.400(1984) MTAs which do not have a
          Distinguished Name, the RFC 2156 syntax 'mta in
```

          globalid' used in X400-Received: fields can be used. Note,
          however, that not all connections an MTA makes are
          necessarily to another MTA."
        ::= {assocEntry 2}

    assocApplicationProtocol OBJECT-TYPE
        SYNTAX OBJECT IDENTIFIER
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "An identification of the protocol being used for the
          application. For an OSI Application, this will be the
          Application Context. For Internet applications, OID
          values of the form {applTCPProtoID port} or {applUDPProtoID
          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
          usual IANA procedures may be used to register ports for
          new protocols."
        ::= {assocEntry 3}

    assocApplicationType OBJECT-TYPE
        SYNTAX INTEGER {
            uainitiator(1),
            uaresponder(2),
            peerinitiator(3),
            peerresponder(4)}
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "This indicates whether the remote application is some type of
          client making use of this network service (e.g., a Mail User
          Agent) or a server acting as a peer. Also indicated is whether
          the remote end initiated an incoming connection to the network
          service or responded to an outgoing connection made by the
          local application. MTAs and messaging gateways are
          considered to be peers for the purposes of this variable."
        ::= {assocEntry 4}

    assocDuration OBJECT-TYPE
        SYNTAX TimeStamp
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
          "The value of sysUpTime at the time this association was
          started. If this association started prior to the last
          initialization of the network subsystem, then this
          object contains a zero value."

         ::= {assocEntry 5}

    -- Conformance information

    applConformance OBJECT IDENTIFIER ::= {application 3}

    applGroups   OBJECT IDENTIFIER ::= {applConformance 1}
    applCompliances OBJECT IDENTIFIER ::= {applConformance 2}

    -- Compliance statements

    applCompliance MODULE-COMPLIANCE
        STATUS obsolete
        DESCRIPTION
          "The compliance statement for RFC 1565 implementations
           which support the Network Services Monitoring MIB
           for basic monitoring of network service applications.
           This is the basic compliance statement for RFC 1565."
        MODULE
          MANDATORY-GROUPS {applRFC1565Group}
        ::= {applCompliances 1}

    assocCompliance MODULE-COMPLIANCE
        STATUS obsolete
        DESCRIPTION
          "The compliance statement for RFC 1565 implementations
           which support the Network Services Monitoring MIB
           for basic monitoring of network service applications
           and their associations."
        MODULE
          MANDATORY-GROUPS {applRFC1565Group, assocRFC1565Group}
        ::= {applCompliances 2}

    applRFC2248Compliance MODULE-COMPLIANCE
        STATUS deprecated
        DESCRIPTION
          "The compliance statement for RFC 2248 implementations
           which support the Network Services Monitoring MIB
           for basic monitoring of network service applications."
        MODULE
          MANDATORY-GROUPS {applRFC2248Group}
        ::= {applCompliances 3}

    assocRFC2248Compliance MODULE-COMPLIANCE
        STATUS deprecated
        DESCRIPTION
          "The compliance statement for RFC 2248 implementations

```
         which support the Network Services Monitoring MIB for
         basic monitoring of network service applications and
         their associations."
      MODULE
        MANDATORY-GROUPS {applRFC2248Group, assocRFC2248Group}
      ::= {applCompliances 4}

   applRFC2788Compliance MODULE-COMPLIANCE
      STATUS current
      DESCRIPTION
        "The compliance statement for RFC 2788 implementations
         which support the Network Services Monitoring MIB
         for basic monitoring of network service applications."
      MODULE
        MANDATORY-GROUPS {applRFC2788Group}
      ::= {applCompliances 5}

   assocRFC2788Compliance MODULE-COMPLIANCE
      STATUS current
      DESCRIPTION
        "The compliance statement for RFC 2788 implementations
         which support the Network Services Monitoring MIB for
         basic monitoring of network service applications and
         their associations."
      MODULE
        MANDATORY-GROUPS {applRFC2788Group, assocRFC2788Group}
      ::= {applCompliances 6}


   -- Units of conformance

   applRFC1565Group OBJECT-GROUP
      OBJECTS {
        applName, applVersion, applUptime, applOperStatus,
        applLastChange, applInboundAssociations,
        applOutboundAssociations, applAccumulatedInboundAssociations,
        applAccumulatedOutboundAssociations, applLastInboundActivity,
        applLastOutboundActivity, applRejectedInboundAssociations,
        applFailedOutboundAssociations}
      STATUS obsolete
      DESCRIPTION
        "A collection of objects providing basic monitoring of
         network service applications.  This is the original set
         of such objects defined in RFC 1565."
      ::= {applGroups 7}

   assocRFC1565Group OBJECT-GROUP
      OBJECTS {
```

                       assocRemoteApplication, assocApplicationProtocol,
                       assocApplicationType, assocDuration}
                   STATUS obsolete
                   DESCRIPTION
                     "A collection of objects providing basic monitoring of
                      network service applications' associations. This is the
                      original set of such objects defined in RFC 1565."
                   ::= {applGroups 2}

               applRFC2248Group OBJECT-GROUP
                   OBJECTS {
                       applName, applVersion, applUptime, applOperStatus,
                       applLastChange, applInboundAssociations,
                       applOutboundAssociations, applAccumulatedInboundAssociations,
                       applAccumulatedOutboundAssociations, applLastInboundActivity,
                       applLastOutboundActivity, applRejectedInboundAssociations,
                       applFailedOutboundAssociations, applDescription, applURL}
                   STATUS deprecated
                   DESCRIPTION
                     "A collection of objects providing basic monitoring of
                      network service applications. This group was originally
                      defined in RFC 2248; note that applDirectoryName is
                      missing."
                   ::= {applGroups 3}

               assocRFC2248Group OBJECT-GROUP
                   OBJECTS {
                       assocRemoteApplication, assocApplicationProtocol,
                       assocApplicationType, assocDuration}
                   STATUS deprecated
                   DESCRIPTION
                     "A collection of objects providing basic monitoring of
                      network service applications' associations. This group
                      was originally defined by RFC 2248."
                   ::= {applGroups 4}

               applRFC2788Group OBJECT-GROUP
                   OBJECTS {
                       applName, applDirectoryName, applVersion, applUptime,
                       applOperStatus, applLastChange, applInboundAssociations,
                       applOutboundAssociations, applAccumulatedInboundAssociations,
                       applAccumulatedOutboundAssociations, applLastInboundActivity,
                       applLastOutboundActivity, applRejectedInboundAssociations,
                       applFailedOutboundAssociations, applDescription, applURL}
                   STATUS current
                   DESCRIPTION
                     "A collection of objects providing basic monitoring of
                      network service applications. This is the appropriate

          group for RFC 2788 -- it adds the applDirectoryName object
          missing in RFC 2248."
        ::= {applGroups 5}

    assocRFC2788Group OBJECT-GROUP
        OBJECTS {
          assocRemoteApplication, assocApplicationProtocol,
          assocApplicationType, assocDuration}
        STATUS current
        DESCRIPTION
          "A collection of objects providing basic monitoring of
           network service applications' associations. This is
           the appropriate group for RFC 2788."
        ::= {applGroups 6}

    -- OIDs of the form {applTCPProtoID port} are intended to be used
    -- for TCP-based protocols that don't have OIDs assigned by other
    -- means. {applUDPProtoID port} serves the same purpose for
    -- UDP-based protocols. In either case 'port' corresponds to
    -- the primary port number being used by the protocol. For example,
    -- assuming no other OID is assigned for SMTP, an OID of
    -- {applTCPProtoID 25} could be used, since SMTP is a TCP-based
    -- protocol that uses port 25 as its primary port.

    applTCPProtoID OBJECT IDENTIFIER ::= {application 4}
    applUDPProtoID OBJECT IDENTIFIER ::= {application 5}

    END

5. Changes made since RFC 2248

   This revision corrects a few minor technical errors in the
   construction of the network services MIB in RFC 2248 [22]. In
   addition, the applName, applVersion, and applDescription fields have
   been changed from DisplayStrings to SnmpAdminStrings. The reference
   to RFC 1779 has also been updated to RFC 2253, which in turn adds the
   ability for distinguished names to be in the UTF-8 character set.

6. Acknowledgements

   This document is a product of the Mail and Directory Management
   (MADMAN) Working Group. It is based on an earlier MIB designed by S.
   Kille, T. Lenggenhager, D. Partain, and W. Yeong. The Electronic
   Mail Association's TSC committee was instrumental in providing
   feedback on and suggesting enhancements to RFC 1565 [23] that have
   led to the present document.

9. References

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

   [2] Krupczak, C. and J. Saperia, "Definitions of System-Level
        Managed Objects for Applications", RFC 2287, February 1998.

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

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

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

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

   [7] McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Structure of
        Management Information Version 2 (SMIv2)", STD 58, RFC 2578,
        April 1999.

   [8] McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Textual
        Conventions for SMIv2", STD 58, RFC 2579, April 1999.

   [9] McCloghrie, K., Perkins, D. and J. Schoenwaelder, "Conformance
        Statements for SMIv2", STD 58, RFC 2580, April 1999.

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

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

   [12] 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.

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

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

   [15] 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.

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

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

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

   [19] Kille, S., "Mapping between X.400(1988) and RFC 822/MIME", RFC
        2156, January 1998.

   [20] Berners-Lee, T., Masinter, L. and M. McCahill, "Uniform Resource
        Locators (URL)", RFC 1738, December 1994.

   [21] Hoffman, P., Masinter, L. and J. Zawinski, "The mailto URL
        Scheme", RFC 2368, July 1998.

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

   [23] Freed, N. and Kille, "Network Services Monitoring MIB", RFC
        1565, January 1994.

   [29] Postel, J. and J. Reynolds, "Telnet Protocol Specification", STD
        8, RFC 854, RFC 855, May 1983.

8. 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, this MIB does provide passive information about the
   existence, type, and configuration of applications on a given host
   that could potentially indicate some sort of vulnerability. Finally,
   the information MIB provides about network usage could be used to
   analyze network traffic patterns.

   SNMPv1 by itself is not a secure 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/SET (read/change/create/delete) the objects in this MIB.

   It is recommended that the implementers consider the security
   features as provided by the SNMPv3 framework. Specifically, the use
   of the User-based Security Model RFC 2574 [14] and the View-based
   Access Control Model RFC 2575 [17] 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 the objects only to those principals
   (users) that have legitimate rights to indeed GET or SET
   (change/create/delete) them.

9. Author and Chair Addresses

   Ned Freed
   Innosoft International, Inc.
   1050 Lakes Drive
   West Covina, CA 91790
   USA

   Phone: +1 626 919 3600
   Fax: +1 626 919 3614
   EMail: ned.freed@innosoft.com

   Steve Kille, MADMAN WG Chair
   MessagingDirect Ltd.
   The Dome, The Square
   Richmond TW9 1DT
   UK

   Phone: +44 20 8332 9091
   EMail: Steve.Kille@MessagingDirect.com

10. Full Copyright Statement

Acknowledgement