Network Working Group
Request for Comments: 2248
Obsoletes: 1565
Category: Standards Track

N. Freed
Innosoft
S. Kille
ISODE Consortium

January 1998

Network Services Monitoring MIB

Status of this Memo

Copyright Notice

1. 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 the Host Resources MIB at present; development of an additional application MIB is currently underway in the IETF.

2. Table of Contents

3. The SNMPv2 Network Management Framework

The SNMPv2 Network Management Framework consists of seven major components. They are:

- RFC 1902 [1] which defines the SMI, the mechanisms used for describing and naming objects for the purpose of management.
- RFC 1903 [2] defines textual conventions for SNMPv2.
- RFC 1904 [3] defines conformance statements for SNMPv2.
- RFC 1905 [4] defines transport mappings for SNMPv2.
- RFC 1906 [5] defines the protocol operations used for network access to managed objects.
- RFC 1907 [6] defines the Management Information Base for SNMPv2.
- RFC 1908 [7] specifies coexistance between SNMP and SNMPv2.

The Framework permits new objects to be defined for the purpose of experimentation and evaluation.

3.1. Object Definitions

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. Objects in the MIB are defined using the subset of Abstract Syntax Notation One (ASN.1) defined in the SMI. In particular, each object type is named by an OBJECT IDENTIFIER, an administratively assigned name. The object type together with an object instance serves to uniquely identify a specific instantiation of the object. For human convenience, we often use a textual string, termed the descriptor, to refer to the object type.

4. 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.

4.1. 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.

4.2. 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.

4.3. 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.

5. 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 accomodated. 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.

6. Definitions

```
    NETWORK-SERVICES-MIB DEFINITIONS ::= BEGIN

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

application MODULE-IDENTITY
    LAST-UPDATED "9708170000Z"
    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 "9311280000Z"
    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
    STATUS current
    DESCRIPTION
        "A Distinguished Name represented in accordance with
         RFC 1779 [8]."
    SYNTAX DisplayString

-- Uniform Resource Locators are stored in URLStrings.

URLString ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "A Uniform Resource Locator represented in accordance
         with RFC 1738 [10]."
    SYNTAX DisplayString

-- 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
        DisplayString,
    applDirectoryName
        DistinguishedName,
    applVersion
        DisplayString,
    applUptime
        TimeStamp,
    applOperStatus
        INTEGER,
    applLastChange
        TimeStamp,
    applInboundAssociations
        Gauge32,
    applOutboundAssociations
        Gauge32,
    applAccumulatedInboundAssociations
        Counter32,
    applAccumulatedOutboundAssociations
        Counter32,
    applLastInboundActivity
        TimeStamp,
    applLastOutboundActivity
        TimeStamp,
    applRejectedInboundAssociations
        Counter32,
    applFailedOutboundAssociations
        Counter32,
    applDescription
        DisplayString,
    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 DisplayString
    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 DisplayString
    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 accomodated.  '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
       assocation occurs when a 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 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."
    ::= {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
        DisplayString,
    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 DisplayString
    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 1327 [9] syntax
       'mta in globalid' should be used. Note, however, that not
       all connections an MTA 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, the IANA
       maintains a registry 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."
    ::= {assocEntry 3}

assocApplicationType OBJECT-TYPE
    SYNTAX INTEGER {
        ua-initiator(1),
        ua-responder(2),
        peer-initiator(3),
        peer-responder(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 current
    DESCRIPTION
      "The compliance statement for SNMPv2 entities
       which implement the Network Services Monitoring MIB
       for basic monitoring of network service applications."
    MODULE  -- this module
      MANDATORY-GROUPS {applGroup}
    ::= {applCompliances 1}

assocCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
      "The compliance statement for SNMPv2 entities which
       implement the Network Services Monitoring MIB for basic
       monitoring of network service applications and their
       associations."
    MODULE  -- this module
      MANDATORY-GROUPS {applGroup, assocGroup}
    ::= {applCompliances 2}
```

```
-- Units of conformance

applGroup OBJECT-GROUP
    OBJECTS {
      applName, 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."
    ::= {applGroups 1}


assocGroup OBJECT-GROUP
    OBJECTS {
      assocRemoteApplication, assocApplicationProtocol,
      assocApplicationType, assocDuration}
    STATUS current
    DESCRIPTION
      "A collection of objects providing basic monitoring of
       network service applications' associations."
    ::= {applGroups 2}


-- 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
```

7. Changes made since RFC 1565

The only changes made to this document since it was issued as RFC 1565 [11] are the following:

(1) applDescription and applURL fields have been added. These fields are intended to identify and describe the application.

(2) A number of DESCRIPTION fields have been reworded, hopefully making them clearer.

(3) The new "quiescing" state has been added to applOperStatus.

(4) The prose about "dynamic single threaded processes" has been removed -- it was simply too confusing.

(5) Various RFC references have been updated to refer to more recent versions.

(6) The MIB has been renamed from APPLICATION-MIB to NETWORK-SERVICES-MIB. This was done because an application MIB is now under development within the IETF that provides very different functionality from this MIB.

8. 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 [11] that have led to the present document.

9. References

[1] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1902, January 1996.

[2] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1903, January 1996.

[3] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1904, January 1996.

[4] SNMPv2 Working Group, 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.

[5] SNMPv2 Working Group, 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.

[6] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC 1907, January 1996.

[7] SNMPv2 Working Group, Case, J., McCloghrie, K., Rose, M., and S. Waldbusser, "Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework", RFC 1908, January 1996.

[8] Kille, S., "A String Representation of Distinguished Names", RFC 1779, March 1995.

[9] Kille, S., "Mapping between X.400(1988) / ISO 10021 and RFC 822", RFC 1327, May 1992.

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

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

10. Security Considerations

This MIB does not offer write access, and as such cannot be used to actively attack a system. However, this MIB does provide passive information about the existance, 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.

11. 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
ISODE Consortium
The Dome, The Square
Richmond TW9 1DT
UK

Phone: +44 181 332 9091
EMail: S.Kille@isode.com

12. Full Copyright Statement