Internet Draft
Document: draft-barnes-midcom-mib-01.txt

M. Barnes
Nortel Networks
Wes Hardaker
Sparta
D. Harrington
Enterasys Networks
M. Stiemerling
NEC Europe Ltd.

Category: Standards Track
Expires: December 2003

June 2003

Middlebox Communications (MIDCOM) Protocol Managed Objects

Status of this Memo

Copyright Notice

Abstract

This document describes and defines the managed objects for dynamic configuration of middleboxes. The scope of the middleboxes to which these managed objects apply is limited to NATs and Firewalls. However, the MIB module as defined by this document is intended to provide a baseline for the dynamic configuration of other types of middleboxes. The applicability of existing Management Information Base (MIB) modules to the MIDCOM requirements, framework and semantics is described. Additional managed objects are defined to satisfy the entirety of the MIDCOM requirements, framework and semantics, providing a complete MIDCOM MIB for NATs and Firewalls to fully realize the requirements of the MIDCOM protocol.

Table of Contents

Overview

This intent of this document is to define a Management Information base (MIB) for dynamic configuration of middleboxes. The scope of the middleboxes to which this MIB is specifically applied is limited to NATs and Firewalls. However, this MIB is intended to be extensible and provide a baseline for the development of managed objects for configuring other types of middleboxes.

Section 1 provides an overview of the SNMP Management Framework. Section 2 provides further background on SNMP and its applicability to the MIDCOM Protocol Framework, Requirements and semantics.

Section 3 provides a high level overview of some existing MIB modules potentially relevant and reusable, which satisfy the MIDCOM requirements and semantics, and relate to the MIDCOM architecture and framework.

Section 4 provides a detailed discussion of existing MIB modules, defining the level of applicability to the MIDCOM protocol requirements, framework and semantics and re-usability for the MIDCOM MIB.

Section 5 defines the additional MIDCOM specific managed objects required to satisfy some of the requirements and to provide a linkage between the existing MIB modules applicable to MIDCOM.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1. SNMP Management Framework

For a detailed overview of the documents that describe the current Internet-Standard (SNMP) Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580[RFC2580].

2. MIDCOM Overview and SNMP Applicability

The MIDCOM architecture and framework [RFC3303] defines a model in which trusted third parties can be delegated to assist middleboxes in performing their operations, without requiring application intelligence be embedded in the middleboxes. This trusted third party is referred to as the MIDCOM Agent. The MIDCOM protocol is defined between the MIDCOM agent and middlebox.

The SNMP management framework provides functions equivalent to those defined by the MIDCOM framework, although there are a few architectural differences.

For SNMP, application intelligence is captured in MIB modules, rather than in the messaging protocol. MIB modules define a data model of the information that can be collected and configured for managed functionality. The SNMP messaging protocol transports the data in a standardized format without needing to understand the semantics of the data being transferred. The endpoints of the communication understand the semantics of the data.

Traditionally, the SNMP endpoints have been called Manager and Agent. An SNMP manager is an entity capable of generating requests and receiving notifications, and a SNMP agent is an entity capable of responding to requests and generating notifications. As applied to

the MIDCOM framework, the SNMP Manager corresponds to the MIDCOM agent and the SNMP Agent corresponds to the Middlebox.

The MIDCOM protocol is divided into three phases, per section 4 of [RFC3303]:

- Session Setup
- Run-time (involving real-time configuration of the middlebox)
- Session Termination

A MIDCOM session is defined to be a lasting association between a MIDCOM agent and a middlebox. The MIDCOM agent should initiate the session prior to the start of the application. Although the SNMP management framework does not have the concept of a session, session-like associations can be established through the use of managed objects. Requests from the MIDCOM agent to the Middlebox are performed using write access to managed objects defined in MIB modules. The middlebox (SNMP agent) responds to requests by sending an SNMP response message indicating the success or failure of the request. The MIDCOM agent (SNMP manager) MAY verify this information by reading or polling the corresponding managed objects.

The MIDCOM Protocol semantics [MDCSEM] defines two basic transaction types: request transactions and notify transactions. SNMPv3 uses the architecture detailed in [RFC3411], where all SNMP entities are capable of performing certain functions, such as the generation of requests, response to requests, the generation of asynchronous notifications, the receipt of notifications, and the proxy-forwarding of SNMP messages. SNMP is used to read and manipulate a virtual database (the MIB) which is composed of objects representing commands, controls, status, and statistics, which are defined in managed-application-specific MIB modules.

3. SNMP and the MIDCOM data model

This section provides a high level description and levels of abstraction of the categories of data required to satisfy the MIDCOM requirements and semantics as it relates to existing SNMP MIB modules.

Application-specific MIB modules can be defined at varying levels of abstraction. At the lowest level, vendor-specific, device-specific parameters may be defined, for instance, to configure a specific model of firewall. At a higher level, a MIB module may define an abstracted view of firewall functionality that can be used to specify a firewall policy, which an implementation can translate into the necessary parameters to configure the specific model of firewall on which the abstract MIB is implemented. At a higher level yet, a MIB module may define service policies or business policies that end up

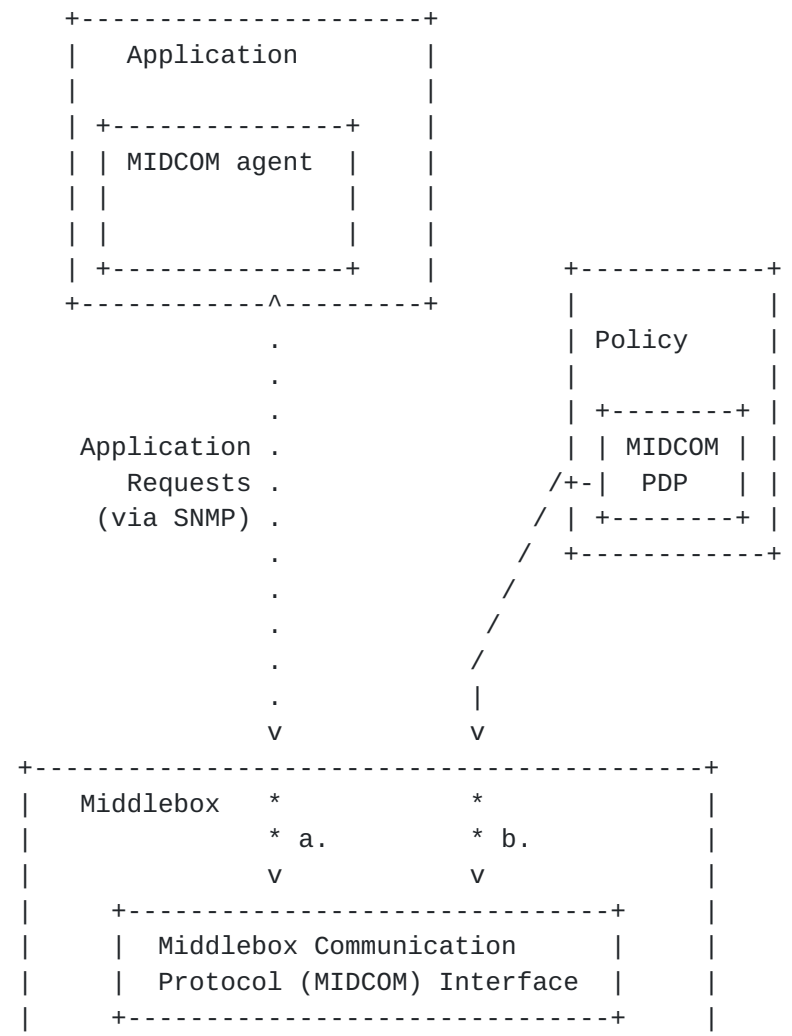
being translated into more detailed instructions, possibly into the

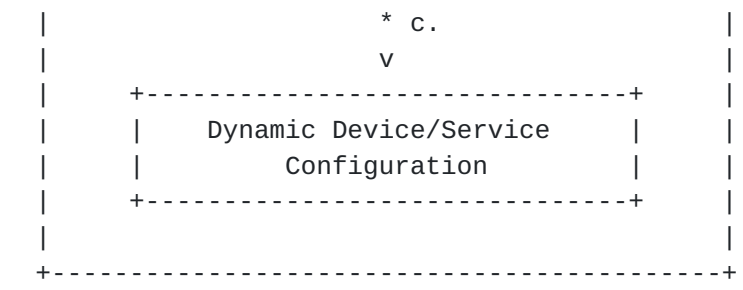
more detailed MIB module data schemas. It is common practice to have one MIB module point to other MIB modules that contain less/more concrete conceptual representations.

SNMP for the MIDCOM protocol can leverage the data schemas of many existing MIB modules designed to permit secure communications, configuration of devices, configuration of services and policy coordination abstractions. The actual specification of the policies is outside the scope of the MIDCOM protocol.

Many existing MIB modules provide monitoring capabilities that can be applied to MIDCOM functionality.

The following diagram (Figure 1) summarizes the potential relevance and reusability of the data schema of existing MIB models to the MIDCOM architecture to satisfy the MIDCOM protocol framework, requirements and semantics:





Legend: .... Middlebox Communication Protocol (MIDCOM)
//// MIDCOM PDP Interface (outside scope of this document)
**** Managed objects relevant to the MIDCOM Interface (with the associated letters referencing the MIB modules potentially applicable summarized below:

a. gaps between existing MIB modules (b and c) and MIDCOM requirements
b. POLICY-BASED-MANAGEMENT-MIB, DIFFSERV-CONFIG-MIB,
c. IPSEC-POLICY-MIB, NAT-MIB, DIFFSERV-MIB

Figure 1: Data relationships relevant to the MIDCOM Interface

3.1 Secure Communications

MIDCOM requirements include mutual authentication, message integrity checking, timeliness checking to prevent replay, message encryption, and authorization controls to ensure only certain agents can modify certain subsets of middlebox configurations. MIDCOM requires secure request-response capabilities and secure notifications.

SNMPv3 is designed to provide secure communications between two end-points. SNMPv3 defines MIB modules to allow the monitoring and configuration of all these security features. They are defined in RFC3411-RFC3418, and RFC3410 provides an overview of these capabilities.

3.2 Device Configuration

SNMP is the most commonly used standardized protocol for remotely monitoring and manipulating the configuration of devices. There are a large number of IETF standard and vendor-specific MIB modules available.

Most IETF standard MIB modules do not provide much configuration support because SNMPv1 and SNMPv2c were non-secure, and it is difficult to standardize abstractions that provide enough information to configure device implementations that require vendor-specific parameters. There are many vendor-specific MIB modules that permit configuration of the vendor's devices.

SNMP MIB modules are definitions of virtual databases with scalars and tables of data. SNMP supports multiple mechanisms to define relationships between entries in different tables. For example, entries in multiple tables are often related by common indices. SNMP uses a standardized hierarchical namespace, so the value of a field in one table can serve as the index into another table.

The ability to define relationships between MIB module tables (including tables in different MIB modules) allows an abstracted configuration policy to point to a vendor-specific configuration MIB module for more detailed instructions.

There are multiple ways to send policies to middleboxes, including SNMP and COPS/PR and RADIUS/Diameter, and most policies are auto-magically converted into low-level configuration commands that set the correct operational parameters to enforce desired behavior.

Some middlebox functionalities are related to physical and logical topologies that are created by dynamically manipulating device configurations. Some MIB modules that can be used for topology configuration would include the 802.1X MIB [81XMIB] and the Interfaces MIB [RFC2863] to enable or disable a physical port or logical interface, the Bridge MIB [BREMIB]to assign interfaces into virtual LANs and to enable port mirroring functionality for IDS usage, the Layer Two Tunneling MIB or IPSec MIB to create topology tunnels for VPNs, and so on.

There are many IETF standard MIB modules that monitor traffic, which can be used to verify that a policy is being enforced. Most "transmission" MIB modules, those that fall under the { MIB-2 transmission } subtree relative to Interfaces MIB entries, provide statistics about traffic going in or out of ports on a device. The Bridge MIB can be used to monitor the amount of traffic being forwarded into or out of virtual LANs, and so on.

3.3 Service Configuration

A middlebox may be able to support multiple types of services, and a MIDCOM agent must determine which services are available and running, and which have stopped running. Middlebox functionalities are applications that run on a middlebox, and there are multiple MIB

modules designed to monitor applications and their operational characteristics. Most of the MIB modules described here are for monitoring only, but could be extended with application-specific MIB modules for configuration and additional monitoring.

The Host Resources MIB [RFC2790] provides monitoring of hardware resources, such as memory and CPU load, and monitors installed applications, running applications, and application performance. These can be used to do capability discovery for a middlebox, and these factors can be important to consider before configuring additional functionality or sessions on a middlebox.

The Network Services Monitoring MIB [RFC2788] module provides objects for monitoring high-level concepts related to network services, such as their current run status and their associations. This MIB works with supplemental service-specific MIB modules, including configuration objects.

The Systems Application MIB [RFC2287] monitors installed applications, running applications, and running processes. The installed application information can be important for determining the actual capabilities of the model and version of firewall installed.

However, MIDCOM is primarily about dynamically configuring middlebox functionality, so MIB modules associated with configuration, specifically any associated with the configuration of firewalls and NATS, are the main focus.

The Diffserv MIB [RFC3289] describes the configuration and management of a Differentiated Services interface in terms of one or more Traffic Conditioning Blocks (TCB), each containing, arranged in the specified order, by definition, zero or more classifiers, meters, actions, algorithmic droppers, queues and schedulers. The "linked-list" approach is very flexible, and could be used to configure some firewall tasks.

The IPSec Policy MIB [IPCMIB] defines objects that could be reused for purposes of filtering service-related traffic and subsequent policy actions.

3.4 Policy Coordination

To properly coordinate policy application, it is necessary to determine if a device has the capabilities needed to effectively enforce a policy, and to coordinate the application of policies according to time constraints, priorities, rule groupings, policy sessions, and so on.

The SNMPCONF working has developed a number of MIB modules designed for the purpose of policy coordination.

Many policies are dependent on factors that are not so much traffic-related as business related. For example, the role that a device serves in the network or the geographic location of a device may impact a policy. The SNMPCONF Policy MIB [PBMMIB] allows an administrator to define roles, and associate them with policies.

The SNMPCONF MIB modules include a policy download table, a policy registration table, and a scheduling function for defining when a policy should be made active and when it should be made dormant. Time schedules can be grouped for easier manipulation, and wildcards are supported. To ease integration with other policy efforts, the schedule table is modeled after the Policy Core Information Model scheduler.

SNMPCONF provides a capabilities table to advertise the functionality available for policy enforcement, including configuration parameters to enable a MIDCOM agent to be notified when new capabilities are installed on a system. Capabilities may be available on some components of a system and not others, such as a board in a chassis, but also may be accessible only in certain logical partitions, such as the community profile (more accurately, the SNMPv3 context) of the super-user.

SNMPCONF defines tracking tables, so an administrator can determine which elements are being controlled by which policies. The MIB also includes debugging tables for logging policy enforcement run-time exceptions. An administrator can disable policies in place, if they desire.

4. Applicability of existing MIB modules

This section summarizes the details of the applicability of existing MIB modules to the MIDCOM data model. As highlighted in Figure 1, the MIDCOM protocol itself is only defined to be the interface from the MIDCOM agent (SNMP manager) to the middlebox or MIDCOM Interface. However, requests from the MIDCOM agent to the MIDCOM Interface must be evaluated against the installed policies and must contain all the data required for the specific device/service configuration. In addition, the session setup reply includes capabilities of the middlebox, several of which relate to policies. Thus, although the Policy interface itself is out of scope of the MIDCOM protocol, the correlation of the policy related data in the form of rules to the data associated with the MIDCOM Interface is imperative. In effect, an instance of the "MIDCOM MIB" comprises the data from the semantics

evaluated against the policy and applied to configure the device/service.

Several of the MIB modules discussed in section 3 were analyzed and and the following were found to have general applicability and varying levels of re-usability for MIDCOM:

- Network Address Translators (NAT) MIB [NATMIB]
- Policy Based Management MIB [PBMMIB]
- IPsec Policy Configuration MIB [IPCMIB]
- Differentiated Services MIB [RFC3289]

4.1 Network Address Translators (NAT) MIB

The NAT MIB module [NATMIB] is intended to be used for configuration as well as monitoring of a device capable of traditional NAT functions. The NAT MIB module appears to meet all of the MIDCOM requirements concerning NAT control. Additional MIB modules, such as those defined by SNMP Policy Based Management MIB (as described in section 4.2), allowing the definition of policy rulesets and grouping of policy rules also required.

4.2 Policy Based Management MIB

This MIB defines managed objects that enable policy-based monitoring and management of SNMP infrastructure. The Policy Based Management MIB defines MIB objects for the following areas: roles, capabilities and time.

[Editor's note: Although the policy interface itself to the middlebox is out of scope for the MIDCOM protocol, the rules associated with the MIB module(s) for MIDCOM are in scope and thus it is anticipated that there is some reusability of the mangaged objects defined by the PBMMIB, rather than of the entire application of this MIB itself. This section will be expanded once more detailed analysis has been completed].

4.3 IPsec Policy Configuration MIB

The IPSEC-POLICY-MIB is a large MIB designed to support IPsec and IKE management in a policy and rule oriented fashion. The MIB module is divided into 3 portions, only one of which would be useful for reuse with the MIDCOM MIB. Specifically, the IPSEC-POLICY-MIB provides a generic mechanism for performing packet processing based on a rule set. Rules within the IPSEC-POLICY-MIB are generic and simply bind a filter to an action. Filters provided within the IPSEC-POLICY-MIB itself are numerous and fairly complete for most common packet filtering usage but externally defined filters (like those that may need to be developed within a MIDCOM specific MIB module) are

supported. The actions encapsulated within the IPSEC-POLICY-MIB are mostly related to IKE and IPsec and thus aren't very useful as applied to MIDCOM. However, actions (like filters) can be externally defined. Compound filter and action sequences can be defined for administrators that need more complex boolean logic or need to chain multiple actions together based on success/failure states. The compound mechanisms are also generic and would let MIDCOM specific MIB elements to be used within the compound bindings if necessary.

[Editor's note: this is an initial analysis; a more detailed analysis to be included once the details are completed].

4.4 Differentiated Services MIB

The Diffserv MIB is a very powerful and flexible MIB module, however, this flexibility is too broad in general for the MIDCOM protocol requirements. In addition, the requirement for NAT support, and specifically policy rule lifetimes in the MIDCOM protocol, further highlight that the Diffserv MIB alone is unsuitable as the MIDCOM MIB Module.

However, the Diffserv model of using different tables for data path elements could be applied to the MIDCOM MIB module. The use of RowPointers as connectors in the Diffserv MIB allows for the simple extension of the MIB. The RowPointers, whether "next" or "specific", may point to Entries defined in other MIB modules. This mechanism can point to other, possibly vendor-specific, configuration MIB modules. In addition, the reuse of some specific definitions out of the DIFFSERV MIB module is worth further consideration for the MIDCOM MIB module, (e.g. the diffServMultiFieldClfrTable).

[Editor's note: Once we start needing to fill in the gaps as highlighted in item a of the diagram in Figure 1, this will be revisited].

4.5 Summary of applicability of existing MIB modules

< To Be Completed >

<Diagram showing these MIB modules as applied to the basic data model>

5. Additional MIDCOM specific managed objects

<MIDCOM specific managed objects may be required to satisfy some of the requirements and to provide a linkage between the existing MIB modules applicable to MIDCOM.>

< To Be Completed >

6. Security Considerations

The MIDCOM requirements [RFC3304] defines the general security requirements for the MIDCOM protocol. The SNMPv3 User-based Security Model (USM, [RFC2574]) satisfies those requirements. USM defines three standardized methods for providing authentication, confidentiality, and integrity. The method to use can be optionally chosen. The methods operate securely across untrusted domains. Additionally, USM has specific built-in mechanisms for preventing replay attacks including unique protocol engine IDs, timers and counters per engine and time windows for the validity of messages.

7. Changes since last version

The following summarizes the major changes made to this document from the previous version (draft-barnes-midcom-mib-00):

- Miscellaneous editorial changes include basic formatting and changing references of mib to MIB, and mibs to MIB modules.
- Removed reference to SNMP proxy functionality as that's not applicable to MIDCOM.
- Updated references to include additional informational references for Diffserv and updated versions on some drafts.
- Incorporated "Protocol" into the title of the document.
- In general, attempted to clarify references to policy to be specific to the rulesets as they apply to a session.
- Some minor re-arranging of text in section 2 to try to improve the readability of the document.
- Clarified that the configuration relevant to MIDCOM is primarily dynamic.
- Removed some of the non-relevant text in sections 3 (eg. References to CLI in the configuration section and some details in the Policy Coordination Section). Totally removed the Policy Specification section since it is out of scope.

Normative References

[RFC3304] R. Swale, P. Mart, P. Sijben, S. Brim, M. Shore, "Middlebox Communications (MIDCOM) Protocol Requirements", RFC 3304, August, 2002.

[RFC3303] P. Srisuresh, J. Kuthan, J. Rosenberg, A. Molitor, A. Rayhan, "Middlebox Communications Architecture and Framework", RFC 3303, August, 2002.

[MDCSEM] Stiemerling, M., Quittek, J., Taylor, T., "MIDCOM Protocol Semantics", draft-ietf-midcom-semantics-02.txt, May, 2003.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC2578] 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.

[RFC2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and S. Waldbusser, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks", STD 62, RFC 3411, November 2002.

[RFC3412] Case, J., Harrington D., Presuhn R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, November 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "SNMPv3 Applications", STD 62, RFC 3413, November 2002.

[RFC3414] Blumenthal, U., and B. Wijnen, "User-based Security Model(USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, November 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, November 2002.

[NATMIB] Raghunarayan, R., Pai, N., Rohit, R., Wang, C., Srisuresh, P., "Definitions of Managed Objects for Network Address Translators (NAT)", draft-ietf-nat-natmib-05.txt, November, 2002.

[PBMMIB] Waldbusser, S., Saperia, J., Hongal, T., "Policy Based Management MIB", draft-ietf-snmpconf-pm-13.txt, March, 2003.

[IPCMIB] Baer, M., Charlet, R., Hardaker, W., Story, R., Wang, C., "IPsec Policy Configuration MIB module", draft-ietf-ipsp-ipsec-conf-MIB-06.txt, March, 2003.

Informative References

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction to Version 3 of the Internet-standard Network Management Framework", 3410, November 2002.

[MDCPEV] Barnes, M., "Middlebox Communications (MIDCOM) Protocol Evaluation", draft-ietf-midcom-protocol-eval-06.txt, November, 2002.

[RFC2287] Krupczak, C. and J. Saperia, "Definitions of System-Level Managed Objects for Applications", RFC 2287, February 1998.

[RFC 2475] Blake, S., et al, "An Architecture for Differentiated Service", RFC 2475, December 1998.

[RFC2564] C. Kalbfleisch, C. Krupczak, R.Presuhn, J. Saperia, "Application Management MIB", May 1999.

[RFC2594] H. Hazewinkel, C. Kalbfleisch, J. Schoenwaelder, "Definitions of Managed Objects for WWW Services", May 1999.

[RFC2788] N. Freed, S. Kille, "Network Services Monitoring MIB", RFC 2788, March 2000.

[RFC2790] S. Waldbusser, P. Grillo, "Host Resources MIB", March 2000.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB using SMIv2", RFC 2863, June 2000.

[RFC3289] Baker, F., Chan, K., Smith, A., "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.

[RFC3290] Bernet, Y., et al, "An Informal Management Model for Differentiated Services Routers", RFC 3290, May 2002.

[DPCMIB] Hazewinkel, H, Partain, D., "The Differentiated Services Configuration MIB", draft-ietf-snmpconf-diffpolicy-05.txt, June 2002.

[BRGMIB] Norseth, K.C. and Bell, E., "Definitions of Managed Objects for Bridges", draft-ietf-bridge-bridgeMIB-smiv2-04.txt, October 2002.

[BREMIB] Ngai, V., "Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions", draft-ietf-bridge-ext-v2-01.txt, September 2002.

[81xMIB] Norseth, K.C. "Definitions for Port Access Control (IEEE 802.1X) MIB", draft-ietf-bridge-8021x-01.txt, February, 2003.

Acknowledgements

The authors would like to thank Randy Presuhn and Pyda Srisuresh for their comments and feedback on the initial version of this document.

Authors' Address

Mary Barnes
Nortel Networks
2380 Performance Drive
Richardson, TX 75082
USA

Phone: 1-972-684-5432
Email: mbarnes@nortelnetworks.com

Wes Hardaker
<to be completed>
USA

Phone:
EMail: hardaker@tislabs.com

David Harrington, Co-chair SNMPv3 WG
Enterasys Networks
35 Industrial Way
Rochester, NH 03867-5005
USA

Phone: +1 603-337-2614
EMail: dbh@enterasys.com

Martin Stiemerling
NEC Europe Ltd.
Network Laboratories
Adenauerplatz 6
69115 Heidelberg
Germany

Phone: +49 6221 90511-13
Email: stiemerling@ccrle.nec.de

Full Copyright Statement