CHAPTER 1

Cisco 10000 Series Router MIB Overview

This chapter provides an overview of the Cisco 10000 Series enhanced MIB management feature. It includes the following sections:

Benefits of MIB Enhancements

The Cisco 10000 Series enhanced MIB management feature allows the router to be managed through the Simple Network Management Protocol (SNMP). The feature also expands the number of Management Information Bases (MIBs) included with the router. See the "SNMP Overview" section on page 1-5 for more information about SNMP and MIBs.

Using the enhanced management feature, you can:

- Manage and monitor Cisco 10000 resources through an SNMP-based network management system (NMS)
- Use SNMP **set** and **get** requests to access information in router MIBs
- Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers

Other benefits include:

- A standards-based technology (SNMP) for monitoring faults and performance on the router
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3)
- Notification of faults, alarms, and conditions that might affect services
- The ability to aggregate fault and alarm information for multiple entities
- A way to access router information other than through the command line interface (CLI)

MIB Versions for 12.2SB Software Release

The string in the table indicates the date and time that the module was most recently modified. The format is YYMMDDHHMMZ or YYYYMMDDHHMMZ

where:

- YY—last two digits of year (only years between 1900-1999)
- YYYY—last four digits of the year (any year)
- MM—month (01 through 12)
- DD—day of month (01 through 31)
- HH—hours (00 through 23)
- MM—minutes (00 through 59)
- Z—denotes GMT (the ASCII character Z)

Note For example, 9502192015Z and 199502192015Z represent 8:15pm GMT on 19 February 1995. Years after 1999 must use the four digit year format. Years 1900-1999 may use the two or four digit format.

Unless otherwise indicated, each MIB is included in all software images for the indicated release. In some cases, MIBs that are included in the software image are not actually supported or are only partially supported. See the individual section for each MIB for more details.

Note The detailed documentation in the MIB guide is only valid for MIBs that have not changed since Cisco software release 12.3(7)XI1.

Table 1-1 lists the MIB versions that are supported in the 12.3(7)XI1, 12.2SB REL3, and 12.2SB REL4 software releases.

Note If not specifically mentioned, the implementation is the same as the previous software release

Table 1-1 Cisco 10000 Series Routers Supported MIB Versions

MIB Name	MIB Versions for 12.3(7)XI1	MIB Versions for 12.2SB REL3	MIB Versions for 12.2(4th)SB
ATM-MIB	9406072245Z	9406072245Z	9406072245Z
ATM-FORUM-ADDR-REG-MIB	9606200322Z	9606200322Z	Not found in REL4
ATM-FORUM-MIB	9606200322Z	9606200322Z	Not found in REL4
BGP4-MIB	9405050000Z	9405050000Z	9405050000Z
CISCO-AAA-SERVER-MIB	2000012000000Z	200001200000Z	200001200000Z
CISCO-AAA-SESSION-MIB	9911160000Z	9911160000Z	200603210000Z
CISCO-AAL5-MIB	9611150000Z	200309220000Z	200309220000Z
CISCO-ATM-EXT-MIB	9706200000Z	200301060000Z	200301060000Z
CISCO-BGP4-MIB			200302240000Z
CISCO-BULK-FILE-MIB	200108220000Z	9810291700Z	200108220000Z
CISCO-CDP-MIB	9812100000Z	9812100000Z	200503210000Z
CISCO-CEF-MIB			200601300000Z

Table 1-1 Cisco 10000 Series Routers Supported MIB Versions (continued)

MIB Name	MIB Versions for 12.3(7)XI1	MIB Versions for 12.2SB REL3	MIB Versions for 12.2(4th)SB
CISCO-CLASS-BASED-QOS-MIB	200307240000Z	200404120000Z	200404120000Z
CISCO-CONFIG-COPY-MIB	200205300000Z	9701150000Z	200403170000Z
CISCO-CONFIG-MAN-MIB	9511280000Z	9511280000Z	9511280000Z
CISCO-ENTITY-ALARM-MIB	9907062150Z	9907062150Z	9907062150Z
CISCO-ENTITY-ASSET-MIB	9906021600Z	200207231600Z	200207231600Z
CISCO-ENTITY-EXT-MIB	200104050000Z	200104050000Z	200104050000Z
CISCO-ENTITY-FRU-CONTROL-MIB	200001130000Z	200209150000Z	200310230000Z
CISCO-ENTITY-PFE-MIB	200211271600Z	200211271600Z	200211271600Z
CISCO-ENTITY-VENDOTYPE-OID-MIB	200204051400Z	200204051400Z	200505050930Z
CISCO-ENVMON-MIB	200108240000Z	200207170000Z	200207170000Z
CISCO-FLASH-MIB	200301311234Z	200301311234Z	200301311234Z
CISCO-FRAME-RELAY-MIB	200010130000Z	200005220000Z	200010130000Z
CISCO-FTP-CLIENT-MIB	9710091700Z	9710091700Z	9710091700Z
CISCO-IETF-IP-MIB			200203040000Z
CISCO-IETF-IP-FORWARD-MIB			200201240000Z
CISCO-IETF-PPVPN-MPLS-VPN-MIB-MIB			200304171200Z
CISCO-IMAGE-MIB	9508150000Z	9508150000Z	9508150000Z
CISCO-IP-LOCAL-POOL-MIB	200304032000Z	200304032000Z	200304032000Z
CISCO-IP-STAT-MIB	9707180000Z	200112202300Z	200112202300Z
CISCO-IP-TAP-MIB			200403110000Z
CISCO-IP-URPF-MIB			200411120000Z
CISCO-IPMROUTE-MIB	200012220000Z	200012220000Z	200503070000Z
CISCO-MEMORY-POOL-MIB	9602120000Z	9602120000Z	9602120000Z
CISCO-NETFLOW-MIB			200604200000Z
CISCO-OAM-MIB	9605010000Z	9605010000Z	9605010000Z
CISCO-PIM-MIB	200011020000Z	200011020000Z	200011020000Z
CISCO-PING-MIB	200108280000Z	200108280000Z	200108280000Z
CISCO-PPPOE-MIB	200102200000Z	200102200000Z	200102200000Z
CISCO-PROCESS-MIB	200301220000Z	200301220000Z	200301220000Z
CISCO-PRODUCTS-MIB	200204051400Z	200204051400Z	200505051930Z
CISCO-QINQ-VLAN-MIB			200411290000Z
CISCO-RTTMON-MIB	200305210000Z	200401200000Z	200501040000Z
CISCO-SSG-MIB	200203250000Z	MIB Not Supported	Not found in REL4

Table 1-1 Cisco 10000 Series Routers Supported MIB Versions (continued)

MIB Name	MIB Versions for 12.3(7)XI1	MIB Versions for 12.2SB REL3	MIB Versions for 12.2(4th)SB
CISCO-SYSLOG-MIB	9508070000Z	9508070000Z	9508070000Z
CISCO-TAP2-MIB			200403110000Z
CISCO-VPDN-MGMT-MIB	990414000000Z	990414000000Z	990414000000Z
CISCO-VPDN-MGMT-EXT-MIB	200207080000Z	200207080000Z	200207080000Z
DS1-MIB	9808011830Z	9808011830Z	9808011830Z
DS3-MIB	9808012130Z	9808012130Z	9808012130Z
ENTITY-MIB	9912070000Z	9912070000Z	9912070000Z
ETHERLIKE-MIB	9908240400Z	9912070000Z	9908240400Z
EVENT-MIB	200010160000Z	200010160000Z	200010160000Z
EXPRESSION-MIB	9802251700Z	9802251700Z	9802251700Z
IF-MIB	9611031355Z	9611031355Z	9611031355Z
IGMP-MIB	9712180000Z	9712180000Z	9712180000Z
IPMROUTE-MIB	9902080000Z	9902080000Z	Not found in REL4
MPLS-LDP-MIB	200003041200Z	200108161200Z	200108161200Z
MPLS-LSR-MIB	200004261200Z	200004261200Z	200004261200Z
MPLS-TE-MIB	200011211200Z	200011211200Z	200011211200Z
MPLS-VPN-MIB	200110151200Z	200110151200Z	200110151200Z
MSDP-MIB	9912160000Z	9912160000Z	9912160000Z
NOTIFICATION-LOG-MIB	200011270000Z	200011270000Z	200011270000Z
PIM-MIB	200009280000Z	200009280000Z	200009280000Z
RFC1213-MIB	9606111939Z	9606111939Z	9606111939Z
RFC1253-MIB	9511170836Z	9511170836Z	Not found in REL4
RFC1315-MIB	9511170836Z	9511170836Z	9511170836Z
SNMP-FRAMEWORK-MIB	9901190000Z	9901190000Z	9901190000Z
SNMP-MPD-MIB	9905041636Z	9905041636Z	9905041636Z
SNMP-NOTIFICATION-MIB	9808040000Z	9808040000Z	9808040000Z
SNMP-PROXY-MIB	9808040000Z	9808040000Z	9808040000Z
SNMP-TARGET-MIB	9808040000Z	9808040000Z	9808040000Z
SNMP-USM-MIB	9901200000Z	9901200000Z	9901200000Z
SNMPv2-MIB	9511090000Z	9511090000Z	9511090000Z
SNMP-VACM-MIB	9901200000Z	9901200000Z	9901200000Z
SONET-MIB	9810190000Z	9810190000Z	9810190000Z
TCP-MIB	9411010000Z	9411010000Z	9411010000Z
UDP-MIB	9411010000Z	9411010000Z	9411010000Z

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has three parts:

- An SNMP manager—A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a network management system (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).
- An SNMP agent—A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent (see the "Enabling SNMP Support" section on page 2-3).
- A Management Information Base

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or set a value in that SNMP agent.

MIB Description

A Management Information Base (MIB) is a collection of network-management information, organized hierarchically. The MIB consists of collections of managed objects identified by object identifiers. MIBs are accessed using a network-management protocol such as SNMP. A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device, such as a router. Managed objects comprise one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs can contain two types of managed objects:

- Scalar objects—Define a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).
- Tabular objects—Define multiple related object instances that are grouped together in MIB tables (for example, ifTable in the IF-MIB defines the interface entities on the router).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—This function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—This function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP Traps

An SNMP agent can send messages to the SNMP manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host. SNMP notifications can be sent as either *traps* or *informs*. See Chapter 4, "Monitoring Notifications," for information about traps.

The Cisco implementation of SNMP uses the definitions of SNMP traps described in RFC 1215.

SNMP Versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv1—The Simple Network Management Protocol: A full Internet standard, defined in RFC 1157. Security is based on community strings.
- SNMPv2c—The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
  - Message integrity—Ensuring that a packet has not been tampered with in transit.
  - Authentication—Determining that the message is from a valid source.
  - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMPv1 and SNMPv2c

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address Access Control List and password.

SNMPv2c support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported:

- No such object exceptions
- No such instance exceptions
- End of MIB view exceptions

SNMPv3

SNMPv3 provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SNMP Security Models and Levels

Table 1-2 describes the security models and levels provided by the different SNMP versions.

Table 1-2 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v2c	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v3	noAuthNoPriv	User name	No	Uses match on user name for authentication.
	authNoPriv	MD5 or SHA	No	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm.
	authPriv	MD5 or SHA	DES	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. Also provides DES 56-bit encryption based on CBC-DES (DES-56) standard.

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Requests For Comments

MIB modules are written in the SNMP MIB module language, and are typically defined in Request For Comments (RFC) documents submitted to the Internet Engineering Task Force (IETF). RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole. Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (http://www.isoc.org and http://www.ietf.org).

We provide private MIB extensions with each Cisco system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices. Top-level MIB OIDs are assigned by standards organizations such as ISO and ITU, while lower-level OIDs are assigned by associated organizations such as the Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.*xyz*-MIB represents the *xyz*-MIB whose location in the MIB hierarchy is as follows. Note that the numbers in parentheses are included only to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).*nn*-MIB

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1).

For a list of OIDs assigned to MIB objects, go to the following URL:

ftp://ftp.cisco.com/pub/mibs/oid/

Related Information and Useful Links

The following URL provides access to general information about Cisco MIBs. Use the links on this page to access MIBs for download, and to access related information (such as application notes and OID listings).

- http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TAC Information and FAQs

The following URLs provide access to SNMP information developed by the Cisco Technical Assistance Center (TAC):

- http://www.cisco.com/warp/public/477/SNMP/index.html is the Cisco TAC page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.

SNMP Configuration Information

The following URLs provide information about configuring SNMP:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/cfun_vcg.htm provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/index.htm provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.