CHAPTER 1

Cisco CMTS Router MIB Overview

This chapter provides an overview of the Cisco Cable Modem Termination System (CMTS) router. This chapter contains the following topics:

- MIB Description, page 1-1
- Benefits of MIB Enhancements, page 1-2
- MIB Dependencies, page 1-2
- MIB Types, page 1-3
- Object Identifiers, page 1-3
- SNMP Overview, page 1-4
- Related Information and Useful Links, page 1-7

MIB Description

A Management Information Base (MIB) is a collection of information that can be managed by the SNMP manager. The objects in a MIB are organized and identified by object identifiers (OID) that are defined by the IETF and other organizations. Cisco's implementation of SNMP uses MIBs that conform to the MIB II definition that is described in RFC 1213.

Objects can refer to a physical device (such as a line card or clock card or shared port adapter), a software parameter (such as an IP address or operation mode), or a run-time statistic (such as number of packets passed or temperature). When the device contains multiple objects of the same type, it appends a unique instance number to the end of the OID, so that the SNMP manager and agent can distinguish between the different objects.

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 interfaces on the router). Each row in a MIB table describes all of the parameters for a particular object (such as IP address, clock speed, number of ports, and so forth). SNMP managers can read or set all of the information in a row with one request.

  Typically, each row in a table is identified by a unique index number. Depending on the table, this index either could reflect a physical attribute (such as the slot number in a chassis or port number on a card) or it could be an arbitrary number (such as is used for tables that list error messages or packet statistics).

Each row also has a status object that shows whether the row is created, activated, deactivated, or deleted. When an SNMP manager creates a new row, it typically sets the row's status to create and then populates the row with the desired parameters. The SNMP agent does not use the objects in a row until the SNMP manager sets the row's status to activate. This ensures that the SNMP agent does not try to use a row's parameters until the SNMP manager has finished creating the row and entered all of the row's required parameters.

Benefits of MIB Enhancements

The Cisco CMTS uBR router enhanced 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.

Using the Cisco CMTS uBR router enhanced management feature, you can:

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

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
- A way to access router information other than through the command line interface (CLI)

MIB Dependencies

The SNMP specifications define MIBs in a highly structured hierarchical format, in which MIBs that are lower in the hierarchy use objects that are defined by MIBs higher up in the hierarchy. Each MIB includes a section titled "IMPORTS" that lists the objects it uses that are defined by other MIBs.

For example, the IF-MIB, which defines standard objects for router interfaces, uses the following IMPORT block:

```
IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32, Counter64,
    Integer32, TimeTicks, mib-2,
    NOTIFICATION-TYPE                       FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, DisplayString,
    PhysAddress, TruthValue, RowStatus,
    TimeStamp, AutonomousType, TestAndIncr   FROM SNMPv2-TC
    MODULE-COMPLIANCE, OBJECT-GROUP,
    NOTIFICATION-GROUP                      FROM SNMPv2-CONF
    snmpTraps                               FROM SNMPv2-MIB
    IANAifType                              FROM IANAifType-MIB;
```

This section shows that the IF-MIB uses objects that are defined by the SNMPv2-SMI, SNMPv2-TC, SNMPv2-CONF, SNMPv2-MIB, and IANAifType-MIB MIBs. To use the IF-MIB with your SNMP management software, you must load these other MIBs as well.

Typically, most SNMP managers use the IMPORT blocks in the MIBs to automatically determine the order in which the MIBs must be loaded. However, if you are manually loading MIBs, you must do so in the proper order.

To determine the dependencies among MIBs, you can use the "View and Download MIBs" tool, which is part of the SNMP Object Navigator on the Cisco IOS MIB Tools page. This URL takes you to the MIB Locator:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

MIB Types

MIBs on the Cisco CMTS can be arranged in the following categories:

- SNMP standard MIBs—Part of the SNMPv1, SNMPv2c, and SNMPv3 specifications and must be supported by any agent supporting SNMP network management. These MIBs provide the framework for SNMP management, defining common objects and interfaces.
- Internet standard MIBs—Provide generic definitions for objects that provide information about commonly used protocols, such as IP, TCP, and Internet Control Message Protocol (ICMP). These MIBs are typically defined by the IETF as Internet-Drafts and Request for Comments (RFCs).
- Cisco platform and network-layer enterprise MIBs—Provide information that is specific to Cisco platforms. These MIBs can extend standard MIBs by providing additional related information, or they can provide information about features that are specific to Cisco platforms. Typically, the same Cisco-specific MIB is used on all Cisco platforms that implement the MIB's particular feature. These MIBs are also typically updated whenever the related feature is updated in the Cisco IOS software.
- Cable-specific MIBs—Provide information about the cable interfaces and related information on the Cisco CMTS platforms. These MIBs can be divided into the following subcategories:
  - DOCSIS-specified MIBs—Defined by CableLabs, which created and maintains the DOCSIS specification. When the DOCSIS specifications have been finalized, these MIBs are also submitted to the IETF and are eventually released as RFCs. These MIBs can also include other services, such as DOCSIS Set-Top Gateway (DSG), as CableLabs continues to develop specifications for these additional cable services.
  - Cisco-specific cable MIBs—Provide extensions to the DOCSIS MIBs for features that are specific to Cisco platforms.
- Deprecated MIBs—Supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network management applications and scripts should convert to the replacement MIBs as soon as possible, because deprecated MIBs could be removed without notice.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed router or other network device. All OIDs are arranged in a hierarchical order, with top-level OIDs assigned by standards organizations such as IETF, ISO, and ITU. Lower-level OIDs are assigned by individual vendor organizations, such as Cisco Systems.

Each level in an OID is assigned both a number and a name. The hierarchical structure of the OIDs allow for easy translation between the number and name forms of an OID.

For example, SNMP standard MIBs that are intended for use by all vendors typically start with "1.3.6.1.2.1", which translates as follows:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)

Typically, vendor-specific MIBs have OIDs that start with "1.3.6.1.4.1", which translates as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1)

Cisco Systems was assigned the next OID of "9", so most OIDs for items that are specific to Cisco platforms start with "1.3.6.1.4.1.9":

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9)

For illustrative purposes, the OIDs above are shown with both number and name forms combined. Typically, only the name or number for a level is used. However, names and numbers can be mixed in the same OID. For example, the top-most Cisco-specific OID could also be given as either "1.3.6.1.4.1.cisco" or "iso.org.dod.internet.private.enterprises.9".

To translate OIDs between their name and number format, and to display the location of any OID in the OID tree, you can use the SNMP Object Navigator on the Cisco IOS MIB Tools page. This URL takes you to the MIB Locator:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

For a listing of all of the objects and OIDs that are included in any particular MIB, you can download the text files at the following URL:

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

SNMP Overview

The Cisco CMTS routers can be managed through SNMP, which is an application-layer protocol that provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework has the following main parts:

- An SNMP manager—A system used to control and monitor the activities of network hosts by using SNMP commands. The most common managing system is called a network management system (NMS), which can be either a standalone device that is dedicated to network management, or a workstation that is running network management applications. Many network management applications are available and range from simple, freely available command-line applications to feature-rich, commercial products with sophisticated graphical user interfaces.
- An SNMP agent—A software component in a managed device that maintains the SNMP data and communicates with the SNMP manager. Typically, the agent is configured to respond only to one or more specific SNMP managers, so that unauthorized parties do not have access to the device. On the Cisco CMTS, the Cisco IOS software runs the SNMP agent software, but it does not become active until it is enabled using the command-line interface (CLI).
- Management Information Base (MIB)—Objects that can be managed by SNMP are defined in MIBs, which are ASCII text files in a structured format. MIBs that are standardized for use industry-wide among multiple vendors are created and maintained by organizations such as the Internet Engineering Task Force (IETF) and CableLabs. Vendors, such as Cisco, also create vendor-specific MIBs to manage vendor-specific platforms and features. On the Cisco CMTS, MIBs are part of the Cisco IOS software image. Typically, each new Cisco IOS software release includes MIBs that are new or have been modified.

The SNMP manager communicates with the SNMP agent in the following ways:

- GET requests—The SNMP manager obtains information from the device by sending GET requests to the agent. The manager can obtain this information one object at a time using single GET requests.
- SET requests—The SNMP manager configures the device by sending SET requests to the agent. The manager can configure one item at a time using single SET requests, or it can configure multiple parameters using a BULK-SET request.
- Notifications—The SNMP agent asynchronously informs the manager that specific events have occurred by using a trap or inform message (depending on the version of SNMP being used). The network administrator configures the agent for the types of traps and informs it should send. These can range from purely informational messages, such as traffic statistics, to important messages that warn of critical situations and errors, such as a card failure.

SNMP Notifications

An SNMP agent can notify the 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, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

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

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 the for instructions on how to enable traps on the Cisco CMTS uBR router. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. See Chapter 4, “Monitoring Notifications,” for information about Cisco CMTS uBR router notifications.

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 SNMPv2c (SNMPv2 classic), and uses the community-based security model of SNMPv1. In particular, SNMPv2c adds support for 64-bit counters.

- 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.

Tip We recommend using SNMPv3 wherever possible because of its superior security features.

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 (ACL) and password.

SNMPv2c support includes a retrieval mechanism and more detailed error message reporting to management stations. The 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. SNMPv1 reported all error conditions using a single error code, but SNMPv2c includes a number of expanded error codes that use different error types to distinguish between different kinds of error conditions.

SNMPv2 also reports three different types of exceptions:

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

SNMPv3

SNMPv3 improves security for SNMP communications by using encryption and by defining security models and security levels:

- Encryption—SNMPv3 supports several industry-standard encryption standards, including the Data Encryption Standard (DES).
- Security Model—An authentication strategy for a user and for the group in which the user resides. Different users can be assigned a different security model, depending on the organization's security structure and needs.
- Security Level—Permitted level of security within a security model. SNMPv1 and SNMPv2c used only a two-stage security level: read-only and read-write. SNMPv3 provides a much greater ability to customize the permission levels for different users.

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

Table 1-1 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 SNMPv3.

Note We recommend using SNMPv3 for all SNMP applications, because of its significant security improvements. In addition, SNMPv3 supports 64-bit counters, which are not supported in SNMPv1. If you use SNMPv1, you can not view any objects that are defined as 64-bit counters.

Requests for Comments

MIB modules are typically defined in Request for Comments (**RFC**) documents that have been submitted to the Internet Engineering Task Force (IETF) for formal discussion and approval. 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 first 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.

Related Information and Useful Links

The following URLs provide access to general information about Cisco MIBs. Use these links to access MIBs for download, and to access related information (such as application notes and OID listings).

- http://tools.cisco.com/ITDIT/MIBS/servlet/index

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

Cisco Technical Support Information and FAQs

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

- http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html is the Cisco Technical Support page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a0080094bc0.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.
- http://www.cisco.com/en/US/customer/tech/tk86/tk808/technologies_q_and_a_item09186a0080094cfd.shtml is a list of frequently asked questions (FAQs) about the use of SNMP on DOCSIS cable networks.

SNMP Configuration Information

The Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3 at http://www.cisco.com/en/US/docs/ios/12_3/featlist/cfun_vcg.html provides information about configuring SNMP support and SNMP commands.

Cisco CMTS Documentation

The following documents describe information about configuring the cable-specific parameters on the Cisco CMTS router:

- *Cisco Broadband Cable Command Reference Guide,* at: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *Cisco CMTS Feature Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

Specifications and Standards

The following are standards and specifications that are used on DOCSIS cable networks. Some of these standards define the MIBs and other aspects of network management that are required for DOCSIS networks.

Note Many of these standards do not directly affect SNMP operations, but they define operational modes and parameters that must be understood to be able to interpret many of the tables and objects that are monitored and managed through SNMP.

Standards[1]	Title
DOCSIS Specifications—These specifications describe the operation and behavior of both CMTS and cable modem platforms on a DOCSIS cable network.	
ANSI/SCTE 22-1 200	Data-over-Cable Service Interface Specifications Radio Frequency Interface, version 1.0
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0
CableHome Specifications—These specifications are not implemented on the CMTS platform but might be useful in understanding the behavior of cable modems and CPE devices.	
CH-SP-MIB-QOS-I03-040129	CableHome QOS MIB Specification
CH-SP-MIB-CAP-I05-040129	CableHome CAP MIB Specification
CH-SP-MIB-CDP-I05-040129	CableHome CDP MIB Specification
CH-SP-MIB-CTP-I05-040129	CableHome CTP MIB Specification
CH-SP-MIB-PSDEV-I05-040129	CableHome PSDEV MIB Specification
CH-SP-MIB-SEC-I05-040129	CableHome Security MIB Specification
CL-SP-MIB-CLABDEF-I03-040113	CableLabs Definition MIB Specification

1. Not all supported standards are listed.