



CHAPTER 1

Cisco 7200 Router MIB Overview

This chapter provides an overview of the Cisco 7200 series routers enhanced management feature for the Cisco 7204VXR, the Cisco 7206VXR, and the Cisco 7201 routers. The Cisco 7200 series routers support multiprotocol, multimedia routing and bridging over a wide variety of LAN and WAN interface types.

This chapter includes the following sections:

- [Benefits of MIB Enhancements, page 1-1](#)
- [SNMP Overview, page 1-2](#)
- [Object Identifiers, page 1-6](#)
- [Related Information and Useful Links, page 1-6](#)

Benefits of MIB Enhancements

The Cisco 7200 series routers are high-performance Enterprise Edge LAN/WAN integration and service provider aggregation routers. The enhanced management feature of the Cisco 7200 series router and the Cisco 7201 router improves management capabilities. The feature improves core network management areas such as inventory, asset and fault management, and expands the number of Management Information Bases (MIBs) included with the router. See the [“SNMP Overview” section on page 1-2](#) for more information about SNMP and MIBs.

Furthermore, the Cisco 7201 router provides application-specific features for broadband subscriber aggregation and network application services with high processing performance.

Using the enhanced management feature, you can:

- Manage and monitor Cisco 7200 series resources through an SNMP-based network management system (NMS).
- Use SNMP **set** and **get** commands to access information in Cisco 7200 series router MIBs..
- Reduce the amount of time and system resources required to perform functions such as 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)
- For a complete list of supported port adapters (PA) supported for the Cisco 7200 Series and the Cisco 7201 router, refer to the following documents on Cisco.com:
 - *Cisco 7200 Series Routers Port Adapter Documentation Roadmap*
http://www.cisco.com/en/US/docs/routers/7200/roadmaps/7200_series_port_adapter_doc_roadmap/3530.html
 - *Cisco 7201 Router Port Adapter Documentation Roadmap*
http://www.cisco.com/en/US/docs/routers/7200/roadmaps/7201_port_adapter_doc_roadmap/1366pr.html

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:

- **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).
- **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 2-4](#)).
- **Management Information Base (MIB)**—Collection of network-management information, organized in hierarchical manner.

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 in hierarchical fashion. 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).

- Columnar objects—Defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects, (for example, ifTable in the IF-MIB defines the interface).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—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—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 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.



Note Many commands use the word traps in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

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 [“Enabling SNMP Support”](#) section on page 2-4 for instructions on how to enable traps on the Cisco 7200 series router. See [Chapter 4, “Monitoring Notifications,”](#) for information about Cisco 7200 series router 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: An 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 the following security models and security levels:

- **Security model**—Authentication strategy that is set up for a user and the group in which the user resides.
- **Security level**—Permitted level of security within a security model.

A combination of a security model and a security level determines the security mechanism to be 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.

Table 1-1 *SNMP Security Models and Levels (continued)*

Model	Level	Authentication	Encryption	Description
v3	noAuthNoPriv	User name	No	Uses match on user name for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm.
v3	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:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA)
- Enterprise MIB OIDs are assigned by 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 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.mib-2.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/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.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/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a0080094bc0.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/en/US/docs/ios/fundamentals/configuration/guide/12_2sx/cf_12_2sx_book.html provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/ffun_r.html provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.