



CHAPTER 1

Cisco ASR 903 Series Aggregation Services Routers Overview

This chapter provides an overview of the enhanced management feature of the Cisco ASR 903 Series Aggregation Services Routers. This chapter contains the following topics:

- [Benefits of MIB Enhancements, page 1-2](#)
- [SNMP Overview, page 1-2](#)
- [Object Identifiers, page 1-2](#)

MIB Description

A MIB is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces and are 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).
- **Columnar objects**—Define multiple related objects such as zero, one, or more instances at any point in time that are grouped together in MIB tables (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.

Benefits of MIB Enhancements

The Cisco ASR 903 Series 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. For more information about SNMP and MIBs, see “[SNMP Overview](#)” section on page 1-2 .

The Cisco ASR 903 Series Router enhanced management feature can be used to:

- Manage and monitor Cisco ASR 903 Series Router resources through an SNMP-based network management system (NMS)
- Access information using SNMP **set** and **get** requests in Cisco ASR 903 Series 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)

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 with the location in the MIB hierarchy as follows. Note that the numbers in parentheses are included 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/>

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 2-3).
- **Management Information Base (MIB)**—MIB is a database of the objects that can be managed on a device.

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.

SNMP Notifications

An SNMP agent can notify 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, 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*. For more information, see [“Enabling Notifications”](#) section on page 4-2. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. For more information about Cisco ASR 903 Series Router traps, see [Chapter 4](#), [“Enabling Notifications.”](#)

SNMP Versions

Cisco IOS XE 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 report the error type. Three kinds of exceptions are also reported:

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

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 the security mechanism 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	Username	No	Uses match on username 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.

The SNMP agent must be configured to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, the Cisco IOS XE software must be configured to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SNMPv3.

RFC

MIB modules are written in the SNMP MIB module language, and are typically defined in 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 website (<http://www.isoc.org>) and IETF website (<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.

TAC Information and FAQs

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

- Cisco TAC page for SNMP at: http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html. It provides links to general SNMP information and tips for using SNMP to gather data.

- Frequently Asked Questions (FAQs) about Cisco MIBs at:
http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a0080094bc0.shtml.

SNMP Configuration Information

The following Cisco documents provide information about configuring SNMP:

- Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2, Part 3 System Management, “*Configuring SNMP Support*” at:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/pcf014.html
- Cisco IOS Configuration Fundamentals Command Reference, Release 12.2, Part 3 System Management Commands, “*SNMP Commands*” at:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/pcf014.html