Cisco ASR 903 Series Aggregation Services Router MIB Specifications Guide

November 28, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-15161-04

Cisco ASR 903 Series Aggregation Services Routers MIB Specifications Guide

CONTENTS

Preface

This guide describes the Cisco ASR 903 Series Aggregation Services Routers implementation of the Simple Network Management Protocol (SNMP). SNMP provides a set of commands for setting and retrieving the values of operating parameters on the Cisco ASR 903 Series Router. Router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many MIB objects that describe router components and provide information about the status of the components.

This preface provides the following sections:

Revision History

The following Revision History table records technical changes, additions, and corrections to this document. The table shows the release number and document revision number for the change, the date of the change, and a summary of the change.

Cisco IOS XE Release	Part Number	Publication Date
IOS XE 3.8	OL-15161-04	November 2012

Description of Changes

- Added new MIBs:
  - CISCO-DOT3-OAM-MIB
  - CISCO-IETF-MPLS-ID-STD-03-MIB
  - CISCO-IETF-MPLS-TE-EXT-STD-03-MIB
  - CISCO-MPLS-LSR-EXT-STD-MIB
  - CISCO-MPLS-TC-EXT-STD-MIB

Cisco IOS XE Release	Part Number	Publication Date
IOS XE 3.7	OL-15161-03	July 2012

Description of Changes

- Added a new MIB CISCO-STP-EXTENSIONS-MIB.

Cisco IOS XE Release	Part Number	Publication Date
IOS XE 3.6	OL-15161-02	March 2012

Description of Changes

- Added new MIBs:
  - CISCO-CBP-TARGET-MIB
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-SONET-MIB
  - IP-FORWARD-MIB (RFC 4292)
  - SONET-MIB (RFC 2558)
- Updated the MIBs:
  - ENTITY-MIB (RFC 4133)
  - IF-MIB (RFC 2863)
  - IP-MIB (RFC 4293)

Cisco IOS XE Release	Part Number	Publication Date
IOS XE 3.5	OL-15161-01	November 28, 2011

Audience

This guide is intended for system and network administrators who are responsible for configuring and operating the Cisco ASR 903 Series Router and for monitoring its performance on the network.

This guide may also be useful for application developers who are developing management applications for the Cisco ASR 903 Series Router.

Organization

This guide contains the following chapters:

Chapter	Description
Chapter 1, "Cisco ASR 903 Series Aggregation Services Routers Overview."	Provides background information about SNMP and its implementation on the Cisco ASR 903 Series Router.
Chapter 2, "Configuring MIB Support."	Provides instructions for configuring SNMP management support on the Cisco ASR 903 Series Router.
Chapter 3, "Cisco ASR 903 Series Router MIB Specifications."	Describes each MIB included on the Cisco ASR 903 Series Router. In addition, constraints for each MIB are listed to indicate how a MIB is implemented on the router.
Chapter 4, "Monitoring Notifications."	Describes SNMP notifications, traps, and informs supported by the Cisco ASR 903 Series Router. It provides the description of each notification, probable cause, and recommended action.
Appendix A "Using MIBs."	Provides information about how to use SNMP to perform system functions such as bulk-file retrieval.

Terminology and Definitions

This section discusses conventions and terminology used in this guide.

- Alarm—In SNMP, the word *alarm* is commonly misused to mean the same as a trap (see the Trap definition below). *Alarm* represents a condition that causes an SNMP trap to be generated.

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 traps, informs, or both. Use the **snmp-server host** and **snmp-server enable** <*notification*> command to specify whether to send SNMP notifications as traps or informs.

- Element Management System (EMS)—An EMS manages a specific portion of the network. For example, the SunNet Manager, an SNMP management application, is used to manage SNMP-manageable elements. Element Managers may manage asynchronous lines, multiplexers, Private Automatic Branch Exchange (PABX), proprietary systems, or an application.
- Inform—Reliable SNMP notifications that are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps. The SNMP Inform mechanism can be used when a reliable fault reporting system is required.
- Lawful Intercept (LI)—The term used to describe the process by which law enforcement agencies conduct electronic surveillance as authorized by judicial or administrative order. Legislation and regulations are increasingly being adopted that require service providers (SPs) to design and implement their networks to explicitly support authorized electronic surveillance.

- Management Information Base (MIB)—The objects that are available in an SNMP-managed device. The information is represented in Abstract Syntax Notation 1 (ASN.1). This is a way of logically grouping data so that it is easily understood by all.
- MIB-II—The successor to MIB-I, which was the original standard SNMP MIB.
- Multiprotocol Label Switching (MPLS)—MPLS is the standardized version of the Cisco original tag-switching proposal. It uses a label-forwarding paradigm (forward packets based on labels).
- Remote Network Monitoring (RMON) MIB—SNMP MIB for remote management of networks. While other MIBs are usually created to support a network device whose primary function is other than management, RMON was created to provide management of a network. RMON is one of the many SNMP-based MIBs that are IETF Standards.
- Simple Network Management Protocol (SNMP)—An application layer protocol that allows you to remotely manage networked devices. The *simple* in SNMP is only in contrast to protocols that are thought to be even more complex than SNMP. SNMP consists of the following components: a management protocol, a definition of management information and events, a core set of management information and events, and a mechanism and approach used to manage the use of the protocol including security and access control.
- Synchronous Optical Network (SONET)—A physical layer interface standard for fiber-optic transmission.
- Trap—A device-initiated SNMP notification message. The contents of the message might be simply informational, but it is mostly used to report real-time trap information. Traps can be used in conjunction with other SNMP mechanisms, as in trap-directed polling.
- User Datagram Protocol (UDP)—A connectionless, non-reliable IP-based transport protocol.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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:

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_item09186a00800 94bc0.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/fcf014.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/frf014.html

CHAPTER 2

Configuring MIB Support

This chapter describes how to configure SNMP and MIB support for the Cisco ASR 903 Series Aggregation Services Routers. It includes the following sections:

Determining MIB Support for Cisco IOS XE Releases

To determine which MIBs are included in the Cisco IOS XE release running on the Cisco ASR 903 Series Router:

Step 1 Go to the Cisco ASR 903 MIBs Support page:

ftp://ftp.cisco.com/pub/mibs/supportlists/asr903/Cisco-ASR-903-MIB-Support-List.html

Step 2 Scroll through the list to find the release you are interested in.

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the Cisco ASR 903 Series Router:

Considerations for Working with MIBs

While working with MIBs, consider the following:

- Mismatches on datatype definitions might cause compiler errors or warning messages. Although Cisco MIB datatype definitions are not mismatched, some standard RFC MIBs do mismatch as in the following example:

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

  This example is considered to be a trivial error and the MIB loads successfully with a warning message.

  The following example is considered as a nontrivial error (even though the two definitions are essentially equivalent), and the MIB is not successfully parsed:

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

  If your MIB compiler treats these as errors, or you want to delete the warning messages, edit one of the MIBs that defines this same datatype so that the definitions match.

- Many MIBs import definitions from other MIBs. If your management application requires MIBs to be loaded, and you experience problems with undefined objects, you might want to load the following MIBs in this order:

  1. SNMPv2-SMI.my
  2. SNMPv2-TC.my
  3. SNMPv2-MIB.my
  4. RFC1213-MIB.my
  5. IF-MIB.my
  6. CISCO-SMI.my
  7. CISCO-PRODUCTS-MIB.my
  8. CISCO-TC.my

- For additional information and SNMP technical tips, go to the Locator page and click **SNMP MIB Technical Tips** or go to the following URL:

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

- For a list of SNMP object identifiers (OIDs) assigned to MIB objects, go to the following URL and click on **SNMP Object Navigator** and follow the links:

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

Note To access this tool, you must have a Cisco.com login account.

- For information about how to download and compile Cisco MIBs, go to the following URL:

  http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800b4cee.shtml

Downloading MIBs

Follow these steps to download the MIBs onto your system if they are not already there:

Step 1 Review the considerations in the "Considerations for Working with MIBs" section.

Step 2 Go to one of the following Cisco URLs. If the MIB you want to download is not there, try the other URL; otherwise, go to one of the URLs in Step 5.

ftp://ftp.cisco.com/pub/mibs/v2

ftp://ftp.cisco.com/pub/mibs/v1

Step 3 Click the link for a MIB to download that MIB to your system.

Step 4 Select **File > Save** or **File > Save As** to save the MIB on your system.

Step 5 You can download industry-standard MIBs from the following URLs:

- http://www.ietf.org
- http://www.broadband-forum.org/

Compiling MIBs

To integrate the Cisco ASR 903 Series Router with an SNMP-based management application, the MIBs for that platform must be compiled. For example, if HP OpenView is running on a UNIX operating system, the Cisco ASR 903 Series Router MIBs must be compiled with the HP OpenView Network Management System (NMS). For instructions, see the NMS documentation.

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco ASR 903 Series Router for SNMP support.

For detailed information about SNMP commands, see the following Cisco documents:

- *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*, Part 3 System Management, "Network Monitoring Using Cisco Service Assurance Agent", available at the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf017.html

- *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2*, Part 3 System Management Commands, "Cisco Service Assurance Agent (SAA) Commands", available at the following URL:

  http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf017.html

To configure the Cisco ASR 903 Series Router for SNMP support:

Step 1 Set up your basic SNMP configuration through the command-line interface (CLI) on the router. Note that these basic configuration commands are issued for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups. (See the preceding list of documents for command and setup information.)

a. Define SNMP based read-only and read-write communities:

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

b. Configure SNMP views (to limit the range of objects accessible to different SNMP user groups):

```
Router (config)# snmp-server view view_name oid-tree {included | excluded}
```

Step 2 Identify (by IP address) the host to receive SNMP notifications from the router:

```
Router (config)# snmp-server host host
```

Step 3 Configure the router to generate notifications. You can use keywords to limit the number and types of messages generated.

```
Router (config)# snmp-server enable traps [notification-type] [notification-option]
```

CHAPTER 3

Cisco ASR 903 Series Router MIB Specifications

This chapter describes the Management Information Base (MIB) on the Cisco ASR 903 Series Aggregation Services Routers. It includes the following sections:

Cisco ASR 903 Series Router MIBs

Each MIB description lists relevant constraints about the implementation of the MIB on the Cisco ASR 903 Series Router platform. Any objects not listed in the table are implemented as defined in the MIB. For detailed MIB descriptions, see the standard MIB.

Note Not all the MIBs included in a Cisco IOS XE software release are fully supported by the Cisco ASR 903 Series Router. Some MIBs are not supported at all. Other MIBs might work, but they have not been tested on the router. In addition, some MIBs are deprecated, but cannot be removed from the software. When a MIB is included in the image, it does not necessarily mean that is supported by the Cisco ASR 903 Series Router platform.

Cisco ASR 903 Series Router MIB Categories

The subsequent tables list the following categories of MIBs in the Cisco ASR 903 Series Router Image on the Cisco ASR 903 Series Router:

- Supported and verified MIBs (tested for Cisco ASR 903 Series Router)—The MIBs exist in the image, the code is implemented, and Cisco has verified that all the supported objects work properly (Table 3-1).
- Supported and unverified MIBs (not tested for Cisco ASR 903 Series Router)—The MIBs exist in the image, the code is implemented, but Cisco has not verified if it is working properly (Table 3-2).
- Unsupported MIBs (no level of support or testing on the Cisco ASR 903 Series Router)—The MIBs may be posted on Cisco.com, but are not present in the image and cannot be queried (Table 3-3).

The MIB version string indicates the date and time that it was most recently modified. The format is YYMMDDHHMMZ or YYYYMMDDHHMMZ, where:

- YY is the last two digits of the year (only years between 1900 and1999).
- YYYY is all four digits of the year (any year).
- MM is the month (01 through 12).
- DD is the day of the month (01 through 31).
- HH is hours (00 through 23).
- MM is minutes (00 through 59).
- Z (the ASCII character Z), denotes Coordinated Universal Time (UTC, formerly Greenwich Mean Time [GMT]). This datatype stores the date and time fields YEAR, MONTH, DAY, HOUR, MINUTE, SECOND, TIMEZONE_HOUR, and TIMEZONE_MINUTE.

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

Note In the following tables you might see the term *Unknown*. This term refers to the MIB that does not have a recorded time stamp indicating the latest modification.

Supported and Verified MIBs

Table 3-1 lists the MIBs that are *supported* and *verified* on the Cisco ASR 903 Series Router in the following Cisco IOS XE software release. The table lists the MIBs, corresponding notification names, and applicable MIB versions.

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
BGP4-MIB (RFC 1657)	bgpEstablished bgpBackwardTransition	9405050000Z
CISCO-BGP-POLICY-ACCOUNTING-MIB	—	200207260000Z
CISCO-BGP4-MIB	cbgpFsmStateChange cbgpBackwardTransition cbgpPrefixThresholdExceeded cbgpPrefixThresholdClear	201009300000Z
CISCO-BULK-FILE-MIB	cbfDefineFileCompletion	200108220000Z
CISCO-CBP-TARGET-MIB	—	200605240000Z
CISCO-CDP-MIB	—	200503210000Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-CEF-MIB	cefResourceFailure cefPeerStateChange cefPeerFIBStateChange cefInconsistencyDetection	200601300000Z
CISCO-CLASS-BASED-QOS-MIB	—	200904240000Z
CISCO-CONFIG-COPY-MIB	ccCopyCompletion	200403170000Z
CISCO-CONFIG-MAN-MIB	ciscoConfigManEvent ccmCLIRunningConfigChanged ccmCTIDRolledOver	200608220000Z
CISCO-DATA-COLLECTION-MIB	cdcVFileCollectionError cdcFileXferComplete	200210300530Z
CISCO-DOT3-OAM-MIB	cdot3OamThresholdEvent cdot3OamNonThresholdEvent	200605310000Z
CISCO-EMBEDDED-EVENT-MGR-MIB	cEventMgrServerEvent cEventMgrPolicyEvent	200611070000Z
CISCO-ENHANCED-MEMPOOL-MIB	cempMemBufferNotify	200812050000Z
CISCO-ENTITY-ALARM-MIB	ceAlarmAsserted ceAlarmCleared	199907062150Z
CISCO-ENTITY-EXT-MIB	—	200811240000Z
CISCO-ENTITY-FRU-CONTROL-MIB	cefcModuleStatusChange cefcPowerStatusChange cefcFRUInserted cefcFRURemoved cefcUnrecognizedFRU cefcFanTrayStatusChange	200810070000Z
CISCO-ENTITY-SENSOR-MIB	entSensorThresholdNotification	200601010000Z
CISCO-ENTITY-VENDORTYPE-OID-MIB	—	200505050930Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-FLASH-MIB	ciscoFlashCopyCompletionTrap ciscoFlashPartitioningCompletionTrap ciscoFlashMiscOpCompletionTrap ciscoFlashDeviceChangeTrap ciscoFlashDeviceInsertedNotif ciscoFlashDeviceRemovedNotif ciscoFlashDeviceInsertedNotifRev1 ciscoFlashDeviceRemovedNotifRev1	201103160000Z
CISCO-FTP-CLIENT-MIB	—	199710091700Z
CISCO-IETF-ISIS-MIB	ciiDatabaseOverload ciiManualAddressDrops ciiCorruptedLSPDetected ciiAttemptToExceedMaxSequence ciiIDLenMismatch ciiMaxAreaAddressesMismatch ciiOwnLSPPurge ciiSequenceNumberSkip ciiAuthenticationTypeFailure ciiAuthenticationFailure ciiVersionSkew ciiAreaM	200508161200Z
CISCO-IETF-MPLS-ID-STD-03-MIB	—	201204080000Z
CISCO-IETF-MPLS-TE-EXT-STD-03-MIB	—	201204080000Z
CISCO-IETF-PW-ATM-MIB	—	200504191200Z
CISCO-IETF-PW-ENET-MIB	—	200209221200Z
CISCO-IETF-PW-MIB	cpwVcDown cpwVcUp	200403171200Z
CISCO-IETF-PW-MPLS-MIB	—	200302261200Z
CISCO-IETF-PW-TDM-MIB	—	200607210000Z
CISCO-IF-EXTENSION-MIB	—	200311140000Z
CISCO-IGMP-FILTER-MIB	—	200111080000Z
CISCO-IMAGE-LICENSE-MGMT-MIB	—	200710160000Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-IMAGE-MIB	—	199508150000Z
CISCO-IPMROUTE-MIB	ciscoIpMRouteMissingHeartBeats	200804010000Z
CISCO-LICENSE-MGMT-MIB	—	200607040000Z
CISCO-MPLS-LSR-EXT-STD-MIB	—	201202220000Z
CISCO-MPLS-TC-EXT-STD-MIB	—	201106160000Z
CISCO-MVPN-MIB	ciscoMvpnMvrfChange	200402231200Z
CISCO-NETSYNC-MIB	—	201010150000Z
CISCO-OSPF-MIB	—	200307180000Z
CISCO-OSPF-TRAP-MIB (draft-ietf-ospf-mib-update-05)	cospfIfConfigError cospfVirtIfConfigError cospfTxRetransmit cospfVirtIfTxRetransmit cospfOriginateLsa cospfMaxAgeLsa cospfNssaTranslatorStatusChange cospfShamLinkStateChange cospfShamLinksStateChange cospfShamLinkNbrStateChange cospfShamLinkConfigError cospfShamLinkAuthFailure cospfShamLinkRxBadPacket cospfShamLinkTxRetransmit	200307180000Z
CISCO-PIM-MIB	ciscoPimInterfaceUp ciscoPimInterfaceDown ciscoPimRPMappingChange ciscoPimInvalidRegister ciscoPimInvalidJoinPrune	200011020000Z
CISCO-PROCESS-MIB	cpmCPURisingThreshold cpmCPUFallingThreshold	201005060000Z
CISCO-PRODUCTS-MIB	—	200505051930Z
CISCO-PTP-MIB	—	201101280000Z
CISCO-RF-MIB	ciscoRFSwactNotif ciscoRFProgressionNotif ciscoRFIssuStateNotifRev1	200803180000Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-RTTMON-MIB	rttMonConnectionChangeNotification rttMonTimeoutNotification rttMonThresholdNotification rttMonVerifyErrorNotification rttMonNotification rttMonLpdDiscoveryNotification rttMonLpdGrpStatusNotification	201102210000Z
CISCO-STP-EXTENSIONS-MIB	—	200503020000Z
CISCO-SONET-MIB	ciscoSonetSectionStatusChange ciscoSonetLineStatusChange ciscoSonetPathStatusChange	200205220000Z
CISCO-SYSLOG-MIB	clogMessageGenerated	199508070000Z
DS1-MIB (RFC 2495)	dsx1LineStatusChange	9808011830Z
ENTITY-MIB (RFC 4133)	entConfigChange	200508100000Z
ENTITY-SENSOR-MIB (RFC 3433)	—	200212160000Z
ENTITY-STATE-MIB	entStateOperEnabled entStateOperDisabled	200511220000Z
EVENT-MIB (RFC 2981)	—	200010160000Z
ETHERLIKE-MIB (RFC 3635)	—	200309190000Z
IEEE8021-CFM-MIB	dot1agCfmFaultAlarm	200810150000Z
IEEE8021-CFM-V2-MIB	—	200810150000Z
IF-MIB (RFC 2863)	linkDown linkUp	9611031355Z
IGMP-STD-MIB (RFC 2933)	—	200009280000Z
IP-FORWARD-MIB (RFC 4292)	—	200602010000Z
IP-MIB (RFC 4293)	—	200602020000Z
IPMROUTE-STD-MIB (RFC 2932)	—	200009220000Z
MPLS-LDP-GENERIC-STD-MIB (RFC 3815)	—	200406030000Z
MPLS-LDP-STD-MIB (RFC 3815)	mplsLdpInitSessionThresholdExceeded mplsLdpPathVectorLimitMismatch mplsLdpSessionUp mplsLdpSessionDown	200406030000Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
MPLS-LSR-STD-MIB (RFC 3813)	mplsXCUp mplsXCDown	200406030000Z
MSDP-MIB	msdpEstablished msdpBackwardTransition	9912160000Z
NOTIFICATION-LOG-MIB (RFC 3014)	—	200011270000Z
OSPF-MIB (RFC 1850)	—	9501201225Z
OSPF-TRAP-MIB (RFC 1850)	ospfIfStateChange ospfVirtIfStateChange ospfNbrStateChange ospfVirtNbrStateChange ospfIfConfigError ospfVirtIfConfigError ospfIfAuthFailure ospfVirtIfAuthFailure ospfIfRxBadPacket ospfVirtIfRxBadPacket ospfTxRetransmit ospfVirtIfTxRetransmit ospfOriginate	9501201225Z
PIM-MIB (RFC 2934)	pimNeighborLoss	200009280000Z
RFC1213-MIB	—	UNKNOWN
RFC2982-MIB	—	200010160000Z
RMON-MIB (RFC 1757)	—	9606111939Z
RSVP-MIB	newFlow lostFlow	9808251820Z
SNMP-COMMUNITY-MIB (RFC 2576)	—	UNKNOWN
SNMP-FRAMEWORK-MIB (RFC 2571)	—	9901190000Z
SNMP-MPD-MIB (RFC 2572)	—	9905041636Z
SNMP-NOTIFICATION-MIB (RFC 2573)	—	9808040000Z
SNMP-PROXY-MIB (RFC 2573)	—	9808040000Z
SNMP-TARGET-MIB (RFC 2573)	—	9808040000Z
SNMP-USM-MIB (RFC 2574)	—	9901200000Z

Table 3-1 MIBs Supported and Verified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
SNMPv2-MIB (RFC 1907)	coldStart warmStart linkDown linkUp authenticationFailure egpNeighborLoss	9511090000Z
SNMPv2-SMI	—	UNKNOWN
SNMP-VIEW-BASED-ACM-MIB (RFC 2575)	—	9901200000Z
SONET-MIB (RFC 2558)	—	9810190000Z
TCP-MIB (RFC 4022)	—	200502180000Z
TUNNEL-MIB (RFC 4087)	—	200505160000Z
UDP-MIB (RFC 4113)	—	200505200000Z

Supported and Unverified MIBs

Table 3-2 lists the MIBs that are *supported* and *unverified* on the Cisco ASR 903 Series Router in the following Cisco IOS XE software release. The table lists the MIBs, corresponding notification names, and applicable MIB versions.

Table 3-2 MIBs Supported and UnVerified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
ATM-MIB	—	9406072245Z
CISCO-ATM-EXT-MIB	—	200301060000Z
CISCO-ATM-IF-MIB	—	200202130000Z
CISCO-ATM-PVC-MIB	—	9711180000Z

Table 3-2 MIBs Supported and UnVerified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-ATM-PVCTRAP-EXTN-MIB	catmIntfPvcUpTrap catmIntfPvcOAMFailureTrap catmIntfPvcSegCCOAMFailureTrap catmIntfPvcEndCCOAMFailureTrap catmIntfPvcAISRDIOAMFailureTrap catmIntfPvcAnyOAMFailureTrap catmIntfPvcOAMRecoverTrap catmIntfPvcSegCCOAMRecoverTrap catmIntfPvcEndCCOAMRecoverTrap catmIntfPvcAISRDIOAMRecoverTrap catmIntfPvcAnyOAMRecoverTrap catmIntfPvcUp2Trap catmIntfPvcDownTrap catmIntfPvcSegAISRDIFailureTrap catmIntfPvcEndAISRDIFailureTrap catmIntfPvcSegAISRDIRecoverTrap catmIntfPvcEndAISRDIRecoverTrap	200303240000Z
CISCO-BCP-MIB	—	200408310000Z
CISCO-CALLHOME-MIB	—	200907140000Z
CISCO-CIRCUIT-INTERFACE-MIB	—	200005090000Z
CISCO-CONTEXT-MAPPING-MIB	—	200503170000Z
CISCO-EIGRP-MIB	—	201004250000Z
CISCO-ERM-MIB	—	200602110000Z
CISCO-ETHERLIKE-EXT-MIB	—	201006040000Z
CISCO-EVC-MIB	cevcEvcCreationNotification cevcEvcDeletionNotification cevcEvcStatusChangedNotification	200805010000Z
CISCO-HSRP-EXT-MIB	—	9808030000Z
CISCO-HSRP-MIB	cHsrpStateChange	9808030000Z
CISCO-IETF-ATM2-PVCTRAP-MIB	atmIntfPvcFailuresTrap	9802030000Z
CISCO-IETF-BFD-MIB	—	200706040000Z
CISCO-IETF-DHCP-SERVER-MIB	—	200703270000Z
CISCO-IETF-DHCP-SERVER-EXT-MIB	—	200703151200Z

Table 3-2 MIBs Supported and UnVerified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-IETF-MPLS-TE-P2MP-STD-MIB	—	200909300000Z
CISCO-IETF-PPVPN-MPLS-VPN-MIB	cMplsNumVrfRouteMaxThreshCleared	200304171200Z
CISCO-IP-STAT-MIB	—	200112202300Z
CISCO-IPSLA-ETHERNET-MIB	—	200801020000Z
CISCO-L2-CONTROL-MIB	—	200306011700Z
CISCO-LAG-MIB	—	200212130000Z
CISCO-MAC-NOTIFICATION-MIB	—	200706110000Z
CISCO-MEMORY-POOL-MIB	—	9602120000Z
CISCO-NHRP-EXT-MIB	—	200811210000Z
CISCO-NTP-MIB	—	200307070000Z
CISCO-PING-MIB	ciscoPingCompletion	200108280000Z
CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	—	200705220000Z
CISCO-RTTMON-ICMP-MIB	—	200508090000Z
CISCO-RTTMON-IP-EXT-MIB	—	200608020000Z
CISCO-RTTMON-RTP-MIB	—	200508090000Z
CISCO-SNMP-TARGET-EXT-MIB	—	200404010000Z
CISCO-TCP-MIB	—	200111120000Z
CISCO-VRF-MIB	—	200912100000Z
ETHER-WIS (RFC 3637)	—	200309190000Z
EXPRESSION-MIB	—	9802251700Z
HC-ALARM-MIB	—	200212160000Z
HC-RMON-MIB	—	9702120000Z
IEEE8021-CFM-V2-MIB	—	200810150000Z
IEEE8023-LAG-MIB	—	200006270000Z
INT-SERV-GUARANTEED-MIB	—	9511030500Z
INTEGRATED-SERVICES-MIB	—	9511030500Z

Table 3-2 MIBs Supported and UnVerified on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
MPLS-L3VPN-STD-MIB (RFC 4382)	mplsL3VpnVrfUp mplsL3VpnVrfDown mplsL3VpnVrfRouteMidThreshExceeded mplsL3VpnVrfNumVrfRouteMaxThreshExceeded mplsL3VpnNumVrfSecIllglLblThrshExcd mplsL3VpnNumVrfRouteMaxThreshCleared	200601230000Z
MPLS-TE-STD-MIB	—	200406030000Z
MPLS-VPN-MIB	mplsVrfIfUp mplsVrfIfDown mplsNumVrfRouteMidThreshExceeded mplsNumVrfRouteMaxThreshExceeded mplsNumVrfSecIllegalLabelThreshExceeded	200110151200Z
NHRP-MIB	—	9908260000Z
RFC2006-MIB (MIP)	—	9606040000Z
RMON2-MIB (RFC 2021)	—	9605270000Z
SMON-MIB	—	9812160000Z
VRRP-MIB	—	200003030000Z

Unsupported MIBs

Table 3-3 lists the MIBs that are *unsupported* and *unverified* on the Cisco ASR 903 Series Router in the following Cisco IOS XE software release.

Table 3-3 MIBs Unsupported on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
ATM2-MIB	—	UNKNOWN
CALISTA-DPA-MIB	—	UNKNOWN
CISCO-AAA-SERVER-MIB	—	UNKNOWN
CISCO-AAA-SESSION-MIB	—	UNKNOWN
CISCO-AAL5-EXT-MIB	—	UNKNOWN
CISCO-ATM-QOS-MIB	—	UNKNOWN

Table 3-3 MIBs Unsupported on the Cisco ASR 903 Series Router

MIB	Notification Name	Revision ID
CISCO-CAR-MIB	—	UNKNOWN
CISCO-ETHER-CFM-MIB	—	UNKNOWN
CISCO-FRAME-RELAY-MIB	—	UNKNOWN
CISCO-IETF-FRR-MIB	—	UNKNOWN
CISCO-IETF-PW-ATM-MIB	—	UNKNOWN
CISCO-IETF-PW-FR-MIB	—	UNKNOWN
CISCO-IGMP-FILTER-MIB	—	UNKNOWN
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	—	UNKNOWN
CISCO-NDE-MIB	—	UNKNOWN
CISCO-NETFLOW-MIB	—	UNKNOWN
CISCO-OTN-IF-MIB	—	UNKNOWN
CISCO-PPPOE-MIB	—	UNKNOWN
CISCO-QINQ-VLAN-MIB	—	UNKNOWN
CISCO-RADIUS-EXT-MIB	—	UNKNOWN
CISCO-SRP-MIB	—	UNKNOWN
CISCO-STACK-MIB	—	UNKNOWN
CISCO-STACKMAKER-MIB	—	UNKNOWN
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	—	UNKNOWN
CISCO-VPDN-MGMT-EXT-MIB	—	UNKNOWN
CISCO-VPDN-MGMT-MIB	—	UNKNOWN
DLSW-MIB	—	UNKNOWN
ETHER-CFM-MIB	—	UNKNOWN
DS3-MIB	—	UNKNOWN
FR-MFR-MIB	—	UNKNOWN
FRAME-RELAY-DTE-MIB	—	UNKNOWN
IMA-MIB	—	UNKNOWN
LLDP-MIB	—	UNKNOWN
NETRANGER	—	UNKNOWN
OLD-CISCO-CHASSIS-MIB	—	UNKNOWN
OLD-CISCO-IP-MIB	—	UNKNOWN
OLD-MPLS-LDP-MIB	—	UNKNOWN
OLD-MPLS-LSR-MIB	—	UNKNOWN
OLD-MPLS-TE-MIB	—	UNKNOWN
RFC1406-MIB	—	UNKNOWN
RFC1407-MIB	—	UNKNOWN

ATM-MIB

The ATM-MIB (RFC 1695) contains the ATM and ATM adaptation layer 5 (AAL5) objects to manage logical and physical entities. It also provides the functionality to manage the relationship between logical and physical entities, such as ATM interfaces, virtual links, cross connects, and AAL5 entities and connections.

BGP4-MIB (RFC 1657)

The BGP4-MIB (RFC 1657) provides access to the implementation information for the Border Gateway Protocol (BGP). The MIB provides:

- Information about the BGP configuration
- Information about BGP peers and messages exchanged within
- Information about the advertised networks

CISCO-AAL5-MIB

The CISCO-AAL5-MIB contains objects to manage performance statistics for ATM adaptation layer 5 (AAL5) virtual channel connections (VCCs). This MIB also contains information such as packets and octets that are received and transmitted on the VCC, which is missing in cAal5VccTable in RFC 1695.

CISCO-ATM-EXT-MIB

The CISCO-ATM-EXT-MIB contains extensions to the Cisco ATM that are used to manage ATM entities. This MIB provides additional AAL5 performance statistics for a virtual channel connection (VCC) on an ATM interface.

MIB Constraints

Table 3-4 lists the constraint that the Cisco ASR 903 Series Router places on the objects in the CISCO-ATM-EXT-MIB.

Table 3-4 CISCO-ATM-EXT-MIB Constraint

MIB Object	Notes
catmxVclOamTable	Not supported.

Note The CISCO-ATM-EXT-MIB has only one table, cAal5VccExtTable. This table augments the aal5VccTable of the CISCO-AAL5-MIB. The cAal5VccExtTable contains additional AAL5 performance parameters.

CISCO-ATM-IF-MIB

The CISCO-ATM-IF-MIB provides the functionality required for an ATM interface configuration.

CISCO-ATM-PVC-MIB

The CISCO-ATM-PVC-MIB provides the functionality to configure a permanent virtual channel (PVC) on an ATM uplink card of a Catalyst 5000 device, and to bind that PVC to a virtual LAN (VLAN).

CISCO-ATM-PVCTRAP-EXTN-MIB

The CISCO-ATM-PVCTRAP-EXTN-MIB contains objects to extend the functionality of the ATM-MIB. This MIB provides additional notifications and traps for permanent virtual circuits (PVCs) on the Cisco ASR 903 Series Router. The CISCO-ATM-PVCTRAP-EXTN-MIB is supplemented by the CISCO-IETF-ATM2-PVCTRAP-MIB.

CISCO-BCP-MIB

The CISCO-BCP-MIB contains objects to manage the Bridge Control Protocol (RFC2878). This MIB is influenced by RFC1474.

CISCO-BGP4-MIB

The CISCO-BGP4-MIB provides access to information related to the implementation of the Border Gateway Protocol (BGP). The MIB provides:

- Information about the BGP configuration
- Information about BGP peers and messages exchanged with them
- Information about advertised networks

CISCO-BGP-POLICY-ACCOUNTING-MIB

The CISCO-BGP-POLICY-ACCOUNTING-MIB contains BGP policy-based accounting information (such as ingress traffic on an interface), which can be used for billing purposes. The MIB provides support for BGP Policy Accounting, which enables you to classify IP traffic into different classes and to maintain statistics for each traffic class.

The MIB contains counts of the number of bytes and packets of each traffic type on each input interface. This information can be used to charge customers according to the route that their traffic travels.

CISCO-BULK-FILE-MIB

The CISCO-BULK-FILE-MIB contains objects to create and delete files of SNMP data for bulk-file transfer.

MIB Constraints

Table 3-5 lists the constraints that the router places on the objects in the CISCO-BULK-FILE-MIB.

Table 3-5 CISCO-BULK-FILE-MIB Constraints

MIB Object	Notes
cbfDefineFileTable	
• cbfDefinedFileStorage	Only *ephemeral* type of file storage is supported. **Note** The ephemeral bulk file created can be moved to a remote FTP server using CISCO-FTP-CLIENT-MIB.
• cbfDefinedFileFormat	Only *bulkBinary* and *bulkASCII* file formats are supported.

Notes: The cbfDefineFileTable has objects that are required for defining a bulk file and for controlling its creation. The cbfDefineObjectTable has information regarding the contents (SNMP data) that go into the bulk file.

When an entry in the cbfDefineFileTable and its corresponding entries in the cbfDefineObjectTable are active, then cbfDefineFileNow can then be set to create. This causes a bulkFile to be created as defined in cbfDefineFileTable and it will also create an entry in the cbfStatusFileTable.

CISCO-CALLHOME-MIB

The CISCO-CALLHOME-MIB contains objects to manage the Call Home feature within the Cisco Call Home architecture framework.

CISCO-CBP-TARGET-MIB

The CISCO-CBP-TARGET-MIB (common class-based policy) contains objects that provide a mapping of targets to which class-based features, such as QoS are applied. A target is a logical interface with which a class-based policy is associated.

MIB Constraints

The configuration objects in the CISCO-CBP-TARGET-MIB are read-only.

Table 3-6 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-CBP-TARGET-MIB.

Table 3-6 CISCO-CBP-TARGET-MIB Constraints

MIB Object	Notes
CbpTargetTable	
• ccbptTargetType	Values are: • genIf(1) • atmPvc(2) • frDlci(3) • controlPlane(4)
• ccbptTargetDir	Values are: • input(2) • output(3)
• ccbptPolicyType	Value is always ciscoCbQos(1) to indicate mapping to CLASS-BASED-QOS-MIB.
• ccbptPolicyId	Contains the cbQosPolicyIndex value for this service-policy.
• ccbptTargetStorageType	Value is always volatile(2).
• ccbptTargetStatus	Value is always volatile(1).
• ccbptPolicyMap	Contains the OID for a cbQosPolicyMapName instance.
• ccbptPolicyInstance	Contains the OID for a cbQosIfType instance.

CISCO-CDP-MIB

The CISCO-CDP-MIB contains objects to manage the Cisco Discovery Protocol (CDP) on the router.

MIB Constraints

Table 3-7 lists the constraints that the router places on the objects in the CISCO-CDP-MIB.

Table 3-7 CISCO-CDP-MIB Constraints

MIB Object	Notes
cdpCtAddressTable	Not supported.
cdpGlobalLastChange	Not supported.
cdpGlobalDeviceIdFormatCpb	Not supported.
cdpGlobalDeviceIdFormat	Not supported.
cdpInterfaceExtTable	Not implemented.

CISCO-CEF-MIB

The CISCO-CEF-MIB contains objects that manage Cisco Express Forwarding (CEF) technology. CEF is the key data plane forwarding path for Layer 3 IP switching technology. The CISCO-CEF-MIB monitors CEF operational data and provides notification when encountering errors in CEF, through SNMP.

MIB Constraints

Table 3-8 lists the constraints that the router places on the objects in the CISCO-CEF-MIB.

Table 3-8 CISCO-CEF-MIB Constraints

MIB Object	Notes
cefCfgAdminState	Read-only. This object is enabled by default.
cefCCCount	Read-only.
cefCCPeriod	Read-only.
cefCCEnabled	Read-only.

Note Cisco Express Forwarding is a high-speed switching mechanism that a router uses to forward packets from the inbound to the outbound interface.

CISCO-CIRCUIT-INTERFACE-MIB

The CISCO-CIRCUIT-INTERFACE-MIB contains objects to configure the circuit description for an interface. The circuit description identifies circuits on interfaces, such as ATM and Frame Relay, and might be used, for example, to correlate performance statistics on the corresponding interfaces.

CISCO-CLASS-BASED-QOS-MIB

The CISCO-CLASS-BASED-QOS-MIB provides read access to quality of service (QoS) configuration information and statistics for Cisco platforms that support the modular QoS CLI.

To understand how to navigate the CISCO-CLASS-BASED-QOS-MIB tables, it is important to understand the relationship between the different QoS objects listed here:

- Match Statement—Indicates the specific match criteria that identifies packets for classification purposes.
- Class Map—Indicates a user-defined traffic class that contains one or more match statements which is used to classify packets into different categories.
- Feature Action—Indicates a QoS feature. Features include policing, traffic shaping, queuing, random detecting, and packet marking. After the traffic is classified, actions are applied to each traffic class.
- Policy Map—Indicates a user-defined policy that associates a QoS feature action to the user-defined class map.
- Service Policy—Indicates a policy map that is attached to an interface.

The MIB uses the following indexes to identify QoS features and distinguish among instances of those features:

- cbQosObjectsIndex—Identifies each QoS feature on the router.
- cbQoSConfigIndex—Identifies a type of QoS configuration. This index is shared by QoS objects that have identical configuration.
- cbQosPolicyIndex—Uniquely identifies a service policy.

QoS MIB information is stored in:

- Configuration instances—This includes all class maps, policy maps, match statements, and feature action configuration parameters. These configuration instances may have multiple identical instances. Multiple instances of the same QoS feature that share a single configuration object is identified by the cbQosConfigIndex.
- Runtime Statistics instances—This includes summary counts and rates sorted by traffic class before and after any configured QoS policies are enforced. In addition, detailed feature-specific statistics are available for select policy map features. Each has a unique run-time instance. Multiple instances of a QoS feature have a separate statistics object. Run-time instances of QoS objects are each assigned a unique identifier (cbQosObjectsIndex) to distinguish among multiple objects with matching configuration.

Note If a class is defined without any action and is mapped to a policy-map, this class and class-default may return incorrect values for the post policy and drop counters represented in the cbQosCMStatsTable.

MIB Constraints

Table 3-9 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-CLASS-BASED-QOS-MIB.

Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints

MIB Object	Notes
cbQosATMPVCPolicyTable	Not implemented.
cbQosFrameRelayPolicyTable	Not implemented.
cbQosInterfacePolicyTable	Not implemented.
cbQosIPHCCfgTable	Not implemented.
cbQosPoliceColorStatsTable	Not implemented.
cbQosPoliceCfgConformColor	Not implemented.
cbQosPoliceCfgExceedColor	Not implemented.
cbQosQueueingCfgTable • cbQosQueueingCfgDynamicQNumber	Not implemented.
cbQosREDCfgTable • cbQosREDCfgECNEnabled	Not implemented.
cbQosTableMapCfgTable	Not implemented.
cbQosTableMapSetCfgTable	Not implemented.
cbQosQueueingClassCfgTable	Not implemented.
cbQosMeasureIPSLACfgTable	Not implemented.
cbQosQueueingCfgPriorityLevel	Not implemented.
cbQosREDClassCfgMaxThresholdUnit	Not implemented.
cbQosREDClassCfgMinThresholdUnit	Not implemented.
cbQosTSCfgRate64	Not implemented.
cbQosREDECNMarkPktOverflow	Not implemented.
cbQosREDECNMarkPkt	Not implemented.
cbQosREDECNMarkPkt64	Not implemented.
cbQosREDECNMarkByteOverflow	Not implemented.
cbQosREDECNMarkByte	Not implemented.
cbQosREDECNMarkByte64	Not implemented.
cbQosREDMeanQSizeUnits	Not implemented.
cbQosREDMeanQSize	Not implemented.
cbQosQueueingCfgPrioBurstSize	Not supported.
cbQosQueueingCfgIndividualQSize	Not supported.
cbQosQueueingCfgDynamicQNumber	Not supported.
cbQosREDECNMarkPktOverflow	Not supported.
cbQosREDECNMarkPkt	Not supported.

Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints

MIB Object	Notes
cbQosREDECNMarkPkt64	Not supported.
cbQosREDECNMarkByteOverflow	Not supported.
cbQosREDECNMarkByte	Not supported.
cbQosREDECNMarkByte64	Not supported.
cbQosSetCfgL2CosInnerValue	Not supported.
cbQosSetDscpTunnelPkt64	Not supported.
cbQosSetPrecedenceTunnelPkt64	Not supported.
cbQosPoliceCfgConformAction	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgConformSetValue	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgExceedAction	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgExceedSetValue	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgViolateAction	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgViolateSetValue	This object is deprecated. Refer to equivalent object in cbQosPoliceActionCfgTable.
cbQosPoliceCfgRate **cbQosPoliceCfgBurstSize** **cbQosPoliceCfgExtBurstSize**	These objects will have zero value when cir (committed information rate) is configured as percent for policing configuration.
cbQosC3plAccountCfgTable	Not implemented.
cbQosC3plAccountStatsTable	Not implemented.

CISCO-CONFIG-COPY-MIB

The CISCO-CONFIG-COPY-MIB contains objects to copy configuration files on the router. For example, the MIB enables the SNMP agent to copy:

- Configuration files to and from the network
- Startup configuration to running configuration and running configuration to startup.
- Startup or running configuration files to and from a local Cisco IOS XE file system.

CISCO-CONFIG-MAN-MIB

The CISCO-CONFIG-MAN-MIB contains objects to track and save changes to the router configuration. The MIB represents a model of the configuration data that exists elsewhere in the router and in peripheral devices. Its main purpose is to report changes to the running configuration through the SNMP notification ciscoConfigManEvent.

CISCO-CONTEXT-MAPPING-MIB

The CISCO-CONTEXT-MAPPING-MIB provides mapping tables that contain the information that a single SNMP agent sometimes needs to support multiple instances of the same MIB. In such cases, network management applications need to know the specific data/identifier values in each context. This is accomplished through the use of multiple SNMP contexts.

CISCO-DATA-COLLECTION-MIB

The CISCO-DATA-COLLECTION-MIB retrieves data periodically when the data displays as a set of discontinuous rows spread across multiple tables. This MIB facilitates data retrieval of tabular objects. This MIB can be used for performance and accounting purposes, where several row instances of a set of objects are polled over a period of time.

The MIB provides the user a way to specify which objects and which instances are required. In addition the MIB provides two ways in which this data can be retrieved.

MIB Constraints

Table 3-10 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-DATA-COLLECTION-MIB. Any MIB object not listed in this table is implemented as defined in the MIB.

Table 3-10 CISCO-DATA-COLLECTION-MIB Constraints

MIB Object	Notes
cdcVFileMgmtTable	Not implemented.
cdcDGTable	Not implemented.
cdcDGBaseObjectTable	Not implemented.
cdcDGInstanceTable	Not implemented.

CISCO-DOT3-OAM-MIB

The CISCO-DOT3-OAM-MIB contains objects that manage the new Ethernet Operations, Administration, and Maintenance (OAM) features introduced by the Ethernet in the first mile task force (IEEE 802.3ah).

MIB Constraints

Table 3-11 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-DOT3-OAM-MIB.

Table 3-11 CISCO-DOT3-OAM-MIB Constraints

MIB Object	Notes
cdot3OamUniqueEventNotificationTx	Read-only.
cdot3OamUniqueEventNotificationRx	Read-only.
cdot3OamDuplicateEventNotificationTx	Read-only.
cdot3OamDuplicateEventNotificationRx	Read-only.
cdot3OamLoopbackControlTx	Read-only.
cdot3OamLoopbackControlRx	Read-only.
cdot3OamVariableRequestTx	Read-only.
cdot3OamVariableRequestRx	Read-only.
cdot3OamVariableResponseTx	Read-only.
cdot3OamVariableResponseRx	Read-only.
cdot3OamOrgSpecificTx	Read-only.
cdot3OamOrgSpecificRx	Read-only.
cdot3OamUnsupportedCodesTx	Read-only.
cdot3OamUnsupportedCodesRx	Read-only.
cdot3OamFramesLostDueToOam	Read-only.
cdot3OamEventLogTimestamp	Read-only.
cdot3OamEventLogOui	Read-only.
cdot3OamEventLogType	Read-only.
cdot3OamEventLogLocation	Read-only.
cdot3OamEventLogWindowHi	Read-only.
cdot3OamEventLogWindowLo	Read-only.
cdot3OamEventLogThresholdHi	Read-only.
cdot3OamEventLogThresholdLo	Read-only.
cdot3OamEventLogValue	Read-only.
cdot3OamEventLogRunningTotal	Read-only.
cdot3OamEventLogEventTotal	Read-only.

CISCO-EIGRP-MIB

The CISCO-EIGRP-MIB defines the tables that are closely aligned with how the router CLI for Enhanced Interior Gateway Protocol (EIGRP) displays information on EIGRP configurations.

CISCO-EMBEDDED-EVENT-MGR-MIB

The CISCO-EMBEDDED-EVENT-MGR-MIB provides descriptions and stores events generated by the Cisco Embedded Event Manager. The Cisco Embedded Event Manager detects hardware and software faults and other events such as OIR for the system.

CISCO-ENHANCED-MEMPOOL-MIB

The CISCO-ENHANCED-MEMPOOL-MIB contains objects to monitor memory pools on all of the physical entities on a managed system. It represents the different types of memory pools that may be present in a managed device. Memory use information is provided to users at three different intervals of time: 1 minute, 5 minutes, and 10 minutes. Memory pools can be categorized into two groups, predefined pools and dynamic pools. The following pool types are currently predefined:

- 1:Processor memory
- 2:I/O memory
- 3:PCI memory
- 4:Fast memory
- 5:Multibus memory
- Other memory

Dynamic pools have a pool type value greater than any of the predefined types listed above. Only the processor pool is required to be supported by all devices. Support for other pool types is dependent on the device being managed.

MIB Constraints

The CISCO-ENHANCED-MEMPOOL-MIB is supported only in the Active RSP module. Table 3-12 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-ENHANCED-MEMPOOL-MIB.

Table 3-12 CISCO-ENHANCED-MEMPOOL-MIB Constraints

MIB Object	Notes
cempMemBufferPoolTable	
• cempMemBufferSize	Read-only.
• cempMemBufferMin	Read-only.
• cempMemBufferMax	Read-only.
• cempMemBufferPermanent	Read-only.
• cempMemBufferTransient	Read-only.
cempMemPoolTable	
• cempMemPoolUsedLowWaterMark	Not implemented.
• cempMemPoolAllocHit	Not implemented.
• cempMemPoolAllocMiss	Not implemented.

Table 3-12 CISCO-ENHANCED-MEMPOOL-MIB Constraints (continued)

MIB Object	Notes
• cempMemPoolFreeHit	Not implemented.
• cempMemPoolFreeMiss	Not implemented.
• cempMemPoolHCShared	Not implemented.
• cempMemPoolHCUsedLowWaterMark	Not implemented.
• cempMemPoolShared	Not implemented.
• cempMemPoolSharedOvrflw	Not implemented.
• cempMemPoolUsedLowWaterMarkOvrflw	Not implemented.
cempMemBufferPoolTable	
• cempMemBufferFreeHit	Not implemented.
• cempMemBufferFreeMiss	Not implemented.

CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB enables the Cisco ASR 903 Series Router to monitor the alarms generated by system components, such as chassis, slots, modules, power supplies, fans, and ports.

CISCO-ENTITY-ALARM-MIB supports these modules:

- A900-IMA8T ASR 900: 8 port 10/100/1000 Ethernet Interface Module
- A900-IMA8S ASR 900: 8 port SFP Gigabit Ethernet Interface Module
- A900-IMA1X ASR 900: 1 port 10GE XFP Interface Module
- A900-IMA16D ASR 900: 16 port T1/E1 Interface Module

All the other interface types are not supported for this release.

For more information on this MIB, see Appendix A, “CISCO-ENTITY-ALARM-MIB.”

MIB Constraints

Table 3-13 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-ENTITY-ALARM-MIB.

Table 3-13 CISCO-ENTITY-ALARM-MIB Constraints

MIB Object	Notes
ceAlarmTable	
• ceAlarmFilterProfile	Not implemented.
• ceAlarmFilterProfileIndexNext	Not implemented.
ceAlarmFilterProfileTable	Not implemented.
ceAlarmDescrTable	
• ceAlarmDescrSeverity	Read-only.

The ENTITY-MIB table, entPhysicalTable, identifies the physical system components in the router. The following list describes the table objects that describe the alarms for the CISCO-ENTITY-ALARM-MIB:

- Physical entity—The component in the Cisco ASR 903 Series Router that generates the alarm.
- ceAlarmDescrVendorType—The object specifies an identifier (typically an enterprise-specific OID) that uniquely identifies the vendor type of those physical entities to which this alarm description applies.
- Alarm severity—Each alarm type defined by a vendor type and employed by the system is assigned an associated severity:
  - Critical—Indicates a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week. For example, online insertion and removal or loss of signal failure when a physical port link is down.
  - Major—Used for hardware or software conditions. Indicates a serious disruption of service or the malfunctioning or failure of important hardware. Requires immediate attention and response of a technician to restore or maintain system stability. The urgency is less than in critical situations because of a lesser effect on service or system performance.
  - Minor—Used for troubles that do not have a serious effect on service to customers or for alarms in hardware that are not essential to the operation of the system.
  - Info—Notification about a condition that could lead to an impending problem or notification of an event that improves operation.

  The syntax values are critical(1), major(2), minor(3), and info(4).
- Alarm description text—Specifies a readable message describing the alarm.
- Alarm type—Identifies the type of alarm that is generated. An arbitrary integer value (0 through 255) uniquely identifies an event relative to a physical entity in the Cisco ASR 903 Series Router.

Table 3-14 lists the alarm descriptions and severity levels for the T1/E1 ports of the Cisco ASR 903 Series Router. The entries for T1/E1 ports mentioned in this table are always populated for ceAlarmDescrTable and ceAlarmDescrVendorType, irrespective of the presence or absence of ports.

Table 3-14 Alarms Supported for T1/E1 ports of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
T1/E1 port	cevPortT1E1	minor	Transmitter is sending remote alarm
	cevPortT1E1	minor	Transmitter is sending AIS
	cevPortT1E1	minor	Transmitter is sending TS16 LOMF alarm
	cevPortT1E1	minor	Receiver has loss of multi-frame in TS16
	cevPortT1E1	minor	Receiver has loss of signal
	cevPortT1E1	minor	Receiver is getting AIS
	cevPortT1E1	minor	Receiver has loss of frame
	cevPortT1E1	minor	Receiver has remote alarm
	cevPortT1E1	minor	Receiver is getting AIS in TS16
	cevPortT1E1	minor	Receiver has remote TS16 LOMF alarm
	cevPortT1E1	minor	Other failure
	cevPortT1E1	minor	Ds1 Physical Port Link Down
	cevPortT1E1	info	Ds1 Physical Port Administrative State Down

Table 3-15 lists the alarm descriptions and severity levels for the Gigabit Ethernet (GE) ports of the Cisco ASR 903 Series Router.

Table 3-15 Alarms Supported for the GE Ports of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
GE port	cevPortGE	critical	Physical port link down.
		info	Physical port administrative state down.
10GE port	cevPort10GigEthPhy	critical	Physical port link down.
		info	Physical port administrative state down.

Note The 10GE Interface Module (IM) card supports only LAN mode.

Table 3-16 lists the alarm descriptions and severity levels for the SFP Container of the Cisco ASR 903 Series Router.

Table 3-16 Alarms Supported for the SFP Container of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescrText
SFP container	cevContainerSFP	Transceiver missing.

Table 3-17 lists the alarm descriptions and severity levels for the IMs of the Cisco ASR 903 Series Router.

Table 3-17 Alarms Supported for the IMs of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
A900-IMA8T	cevIM8pGeCu	major	Unknown state.
A900-IMA8S	cevIM8pGeSFP	major	Boot state.
A900-IMA1X	cevIM1p10GeXfp	major	Disabled.
A900-IMA16D	cevIM16pT1E1	critical	Failed.
		major	Stopped.

Table 3-18 lists the alarm descriptions and severity levels for the Cisco ASR 903 Series Router sensors.

Table 3-18 Alarms Supported for Cisco ASR 903 Series Router Sensors

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Sensor	cevSensor	critical	Faulty Sensor.
		critical	Reading Above Normal (Shutdown).
		critical	Reading Above Normal.
		major	Reading Above Normal.
		minor	Reading Above Normal.
		critical	Reading Below Normal (Shutdown).
		critical	Reading Below Normal.
		major	Reading Below Normal.
		minor	Reading Below Normal.

Note These alarms are not supported for XCVR sensors. The CISCO-ENTITY-SENSOR-MIB can be used to monitor the alarms listed in Table 3-18.

Table 3-19 lists the alarm descriptions and severity levels for the IM containers of the Cisco ASR 903 Series Router.

Table 3-19 Alarms Supported for the IM Container of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
IM bay	cevContainerIMBay	critical	Active card removed OIR alarm.
		critical	Card stopped responding.

Table 3-20 lists the alarm descriptions and severity levels for the Cisco ASR 903 Series Router USB ports.

Table 3-20 Alarms Supported for Cisco ASR 903 Series Router USB Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
USB port	cevPortUSB	critical	Active card removed OIR alarm.
		critical	Card stopped responding.

Table 3-21 lists the alarm descriptions and severity levels for the RSP containers of the Cisco ASR 903 Series Router.

Table 3-21 Alarms Supported for the RSP Container of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RSP container	cevContainerASR900RSP Slot	critical	RSP removed OIR alarm.
		critical	RSP stopped responding.

Table 3-22 lists the alarm descriptions and severity levels for the power supply bay of the Cisco ASR 903 Series Router.

Table 3-22 Alarms Supported for the Power Supply Bay of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Power Supply Bay	cevContainerASR900 PowerSupplyBay	critical	Power supply/Fan module missing.

Table 3-23 lists the alarm descriptions and severity levels for the RSPs of the Cisco ASR 903 Series Router.

Table 3-23 Alarms Supported for the RSP Module of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RSP Module	cevModuleASR903RSP1A	major	Unknown state.
	cevModuleASR903RSP1B	major	Boot state.
		major	Disabled.
		critical	Incompatible
		critical	CPLD incompatible.
		critical	Active RSP CPLD incompatible.
		critical	Failed.
		critical	Cutover.
		major	Secondary failure.
		major	Secondary removed.
		major	Secondary not synchronized.
		critical	No working ESP.
		major	Harddisk Missing.

Note 'Harddisk Missing' and 'No working ESP' alarms are not supported in Cisco ASR 903 Series Router.

The vendor OID for the RSP Module is set to cevModuleUnknownCard for the following conditions:

- Secondary RSP is loaded with the valid image and the RSP module is not operational.
- Software does not understand the hardware subtype of the secondary RSP module.
- Secondary RSP is loaded with an invalid image.

Table 3-24 lists the alarm descriptions and severity levels for the unknown RSP modules of the Cisco ASR 903 Series Router.

Table 3-24 Alarms Supported for the unknown RSP modules of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RSP Module	cevModuleUnknownCard	major	Unknown state.
		major	Boot state.
		major	Disabled.
		critical	Failed.
		critical	Stopped.

Table 3-25 lists the alarm descriptions and severity levels for the power supply module of the Cisco ASR 903 Series Router.

Table 3-25 Alarms Supported for the Power Supply Module of the Cisco ASR 903 Series Router

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Power Supply Modules	cevPowerSupplyASR900 DC500W	critical	Power Supply Failure.

Table 3-26 lists the alarms that the FanTray module of the Cisco ASR 903 Series Router supports.

Table 3-26 Alarms Supported for the Cisco ASR 903 Series Router FanTray Module

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
FanTray Modules	cevFanASR903FanTray	critical	FanTray/Module Failure.
		critical	All Fans Failed.
		critical	Multiple Fan Failures.
		major	Fan 0 to Fan 11 failure.

Note The ceAlarmHistTable contains alarm data asserted or cleared (or both) in the current active RSP. It does not retain the alarms asserted or cleared (or both) in the previous active RSP. The data contained in ceAlarmHistTable is refreshed after a switchover.

CISCO-ENTITY-EXT-MIB

The CISCO-ENTITY-EXT-MIB contains extensions for the processor modules listed in the ENTITY-MIB entPhysicalTable. A processor module is any physical entity that has a CPU, RAM, and NVRAM, and can load a boot image and save a configuration. The extensions in this MIB provide information, such as RAM and NVRAM sizes, configuration register settings, and bootload image name for each processor module.

MIB Constraints

Only the active RP processor is supported in Cisco ASR 903 Series Router. The standby RSP is not managed in this MIB.

Table 3-27 lists the constraints that the router places on the objects in the CISCO-ENTITY-EXT-MIB.

Table 3-27 CISCO-ENTITY-EXT-MIB Constraints

MIB Object	Notes
ceExtConfigRegNext	Read-only.
ceExtSysBootImageList	Read-only.

CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB contains objects to configure and monitor the status of the field replaceable units (FRUs) on the Cisco ASR 903 Series Router listed in the ENTITY-MIB entPhysicalTable. A FRU is a hardware component (such as, a line card and module, fan, or power supply) that can be replaced on site.

MIB Constraints

Table 3-28 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-ENTITY-FRU-CONTROL-MIB.

Table 3-28 CISCO-ENTITY-FRU-CONTROL-MIB Constraints

MIB Object	Notes
cefcModuleTable	
• cefcModuleAdminStatus	Read-only. Always enabled(1) for USB.
• cefcModuleOperStatus	The following values are supported: • unknown(1) • ok(2) • boot(5) • failed(7) • dormant(12) • outOfServiceAdmin(13) Always on(2) for USB.
• cefcModuleResetReason	Implemented for IM Modules only.
• cefcModuleLastClearConfigTime	Not implemented.
• cefcModuleResetReasonDescription	Not implemented.
• cefcModuleStateChangeReasonDescr	Not implemented.
cefcFRUPowerSupplyGroupTable	Not implemented.

Table 3-28 CISCO-ENTITY-FRU-CONTROL-MIB Constraints (continued)

MIB Object	Notes
cefcFRUPowerSupplyValueTable	Not implemented.
cefcFRUPowerStatusTable	
• cefcFRUPowerAdminStatus	always on(1)
• cefcFRUPowerOperStatus	The following values are supported: • always on(2) • failed(8) • onButFanFail(9)
cefcFanTrayStatusTable	
• cefFanTrayOperStatus	always up(2)
cefcIntelliModuleTable	Not implemented.
cefcPhysicalTable	Not implemented.
cefcModuleUpTime	Always zero for USB.

CISCO-ENTITY-SENSOR-MIB

The CISCO-ENTITY-SENSOR-MIB contains objects that support the monitoring of sensors. The MIB is applicable to sensors present in various transceiver modules. This MIB allows to monitor sensor values and thresholds on sensors that are discovered by the ENTITY-MIB.

MIB Constraints

Table 3-29 lists the constraints that the Cisco ASR 903 Series Router places on the CISCO-ENTITY-SENSOR-MIB.

Table 3-29 CISCO-ENTITY-SENSOR-MIB Constraints

MIB Object	Notes
entSensorValueTable	
• entSensorMeasuredEntity	Implemented for all sensors except for transceiver sensors.
entSensorThresholdTable	
• entSensorThresholdRelation	Read-only.
• entSensorThresholdSeverity	Read-only.
• entSensorThresholdValue	Read-only.

MIB Usage Values for Cisco Transceivers

Table 3-30 lists CISCO-ENTITY-SENSOR-MIB sensor objects and their usage values for Cisco ASR 903 Series Router transceivers in the entSensorValueTable and entSensorThresholdTable..

Table 3-30 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco ASR 903 Series Router Transceivers

MIB Sensor Object	Notes
Module Temperature Sensor	
• entSensorType	celsius(8)
• entSensorScale	units(9)
• entSensorPrecision	3
• entSensorStatus	ok(1)
• entSensorValue	Reports most recent measurement seen by the sensor.
• entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object.
• entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds (for example, 60 seconds).
• entSensorMeasuredEntity	0
Tx Supply Voltage Sensor	
• entSensorType	voltsDC(4)
• entSensorScale	milli(8)
• entSensorPrecision	1
• entSensorStatus	ok(1)
• entSensorValue	Reports most recent measurement seen by the sensor.
• entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object.
• entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds (for example, 60 seconds).
• entSensorMeasuredEntity	0
Tx Laser Current Sensor	
• entSensorType	amperes(5)
• entSensorScale	milli(8)
• entSensorPrecision	0
• entSensorStatus	ok(1)
• entSensorValue	Reports most recent measurement seen by the sensor.
• entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object.
• entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds (for example, 60 seconds).
• entSensorMeasuredEntity	0

Table 3-30 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco ASR 903 Series Router Transceivers (continued)

MIB Sensor Object	Notes
Transmit Power Sensor (Optical Tx)	
Receive Power Sensor (Optical Rx)	
• entSensorType	dBm(14)
• entSensorScale	units(9)
• entSensorPrecision	0
• entSensorStatus	ok(1)
• entSensorValue	Reports most recent measurement seen by the sensor.
• entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object.
• entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds (for example, 60 seconds).
• entSensorMeasuredEntity	0

Note The RSPs and power supplies support various sensors. These sensors are supported in the CISCO-ENTITY-SENSOR-MIB.

CISCO-ENTITY-VENDORTYPE-OID-MIB

The CISCO-ENTITY-VENDORTYPE-OID-MIB defines the object identifiers (OIDs) assigned to various Cisco ASR 903 Series Router components. The OIDs in this MIB are used as values for the entPhysicalVendorType field in the entPhysicalTable of the ENTITY MIB. Each OID uniquely identifies a type of physical entity:

- Chassis
- RSP module
- IM Module
- Power Supply Module
- Fan Tray

CISCO-ERM-MIB

The CISCO-ERM-MIB contains objects to manage resources, such as CPU, memory, buffers and so on. The two important scenarios where the Embedded Resource Manager (ERM) framework is used are:

- Resource Depletion—Handles a situation where the system runs out of a finite resource.
- Resource Separation—Shares resources fairly between different entities in the system such that the activity of one entity does not adversely affect others.

CISCO-ETHER-CFM-MIB

The CISCO-ETHER-CFM-MIB defines the managed objects and notifications for Ethernet Connectivity Fault Management (CFM) operation. CFM is an end-to-end per service instance for the Ethernet layer Operations, Administration and Management (OAM) protocol.

CISCO-ETHERLIKE-EXT-MIB

The CISCO-ETHERLIKE-EXT-MIB defines generic objects for the Ethernet-like network interfaces.

MIB Constraints

Table 3-31 lists the constraint that the Cisco ASR 903 Series Router places on the objects in the CISCO-ETHERLIKE-EXT-MIB.

Table 3-31 CISCO-ETHERLIKE-EXT-MIB Constraint

MIB Object	Notes
ceeDot3PauseExtTable	Not Supported.

CISCO-EVC-MIB

The CISCO-EVC-MIB defines the managed objects and notifications describing Ethernet Virtual Connections (EVCs).

MIB Constraints

Table 3-32 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-EVC-MIB.

Table 3-32 CISCO-EVC-MIB Constraint

MIB Object	Notes
cevcEvcUniTable	Not supported.
cevcEvcActiveUnis	Not supported.
ciscoEvcStatusChangedNotification	Not supported.
• cevcEvcOperStatus	Returns unknown as value.

CISCO-FLASH-MIB

The CISCO-FLASH-MIB contains objects to manage flash cards and flash-card operations.

MIB Constraints

Table 3-33 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-FLASH-MIB.

Table 3-33 CISCO-FLASH-MIB Constraints

MIB Object	Notes
ciscoFlashDeviceTable	
• ciscoFlashDeviceInitTime	Not implemented.
• ciscoFlashPhyEntIndex	Not implemented.
ciscoFlashPartitionTable	
• ciscoFlashPartitionFileCount	Not implemented.
• ciscoFlashPartitionChecksumAlgorithm	Not implemented.
• ciscoFlashPartitionUpgradeMethod	Not implemented.
• ciscoFlashPartitionNeedErasure	Not implemented.
• ciscoFlashPartitionFileNameLength	Not implemented.
ciscoFlashFileTable	
• ciscoFlashFileChecksum	Not implemented.
• ciscoFlashFileType	Values not supported: config(2) image(3) crashinfo(5)

Note The index of files stored in USB changes frequently since the files are mounted and unmounted after regular intervals.

Note When both primary and secondary RSPs are up and running, entities for the standby USB flash and Flash disk are not populated for CISCO-FLASH-MIB. Compact Flash is not supported in Cisco ASR 903 Series Router. Therefore, it is not modelled in the CISCO-FLASH-MIB.

Note After the file is copied successfully via TFTP, it takes atleast 50 seconds to reflect the correct file size in the ciscoFlashFileSize object.

CISCO-FTP-CLIENT-MIB

The CISCO-FTP-CLIENT-MIB contains objects to invoke File Transfer Protocol (FTP) operations for network management. This MIB has no known constraints and all objects are implemented as defined in the MIB.

CISCO-HSRP-EXT-MIB

The CISCO-HSRP-EXT-MIB provides an extension to the CISCO-HSRP-MIB which defines the Cisco Hot Standby Router Protocol (HSRP), which is defined in RFC 2281. The extensions cover assigning of secondary IP addresses and modifying an HSRP group's priority.

CISCO-HSRP-MIB

The CISCO-HSRP-MIB contains objects to configure and manage the Cisco Hot Standby Router Protocol (HSRP), which is defined in RFC 2281.

CISCO-IETF-ATM2-PVCTRAP-MIB

The CISCO-IETF-ATM2-PVCTRAP-MIB contains objects that supplement the ATM-MIB. This MIB implements the Virtual Channel Link (VCL) section of the IETF document "draft-ietf-atommib-atm2-11.txt," Section 9 ATM Related Trap Support.

CISCO-IETF-BFD-MIB

The CISCO-IETF-BFD-MIB contains objects to manage the Bidirectional Forwarding Detection (BFD) protocol. BFD detects faults in the bidirectional path between two forwarding engines, including interfaces, data links, and the forwarding engines themselves with potentially very low latency. It operates independently of media, data protocols, and routing protocols.

CISCO-IETF-DHCP-SERVER-MIB

The CISCO-IETF-DHCP-SERVER-MIB contains objects for the entities implementing the server side of the Bootstrap Protocol (BOOTP) and the DHCP for IP version 4 (IPv4). This MIB does not include support for updating Dynamic Domain Name System (DDNS) and DHCP failover protocol.

CISCO-IETF-DHCP-SERVER-EXT-MIB

The CISCO-IETF-DHCP-SERVER-EXT-MIB is an extension of the CISCO-IETF-DHCP-SERVER-MIB.

CISCO-IETF-ISIS-MIB

The CISCO-IETF-ISIS-MIB introduces network management support for the IS-IS routing protocol through the use of IS-IS MIB table entries, MIB objects, and MIB trap notification objects. A new CLI is added to enable SNMP notifications for the objects. Notifications are provided for errors and other significant event information for the IS-IS network.

CISCO-IETF-MPLS-ID-STD-03-MIB

The CISCO-IETF-MPLS-ID-STD-03-MIB contains object definitions for Multiprotocol Label Switching (MPLS) Traffic Engineering in transport networks.

MIB Constraints

Table 3-34 lists the constraints that the router places on the objects in the CISCO-IETF-MPLS-ID-STD-03-MIB.

Table 3-34 CISCO-IETF-MPLS-ID-STD-03-MIB Constraints

MIB Object	Notes
cmplsIdObjects	Read-only.

CISCO-IETF-MPLS-TE-EXT-STD-03-MIB

The CISCO-IETF-MPLS-TE-EXT-STD-03-MIB contains generic object definitions for MPLS Traffic Engineering in transport networks.

MIB Constraints

Table 3-34 lists the constraints that the router places on the objects in the CISCO-IETF-MPLS-TE-EXT-STD-03-MIB.

Table 3-35 CISCO-IETF-MPLS-TE-EXT-STD-03-MIB Constraints

MIB Object	Notes
cmplsTeExtObjects	Read-only.
cmplsTunnelReversePerfBytes	Not implemented.
cmplsTunnelReversePerfPackets	Not implemented.
cmplsTunnelReversePerfErrors	Not implemented.
cmplsTunnelReversePerfHCBytes	Not implemented.
cmplsTunnelReversePerfHCPackets	Not implemented.

CISCO-IETF-MPLS-TE-P2MP-STD-MIB

The CISCO-IETF-MPLS-TE-P2MP-STD-MIB contains objects to manage the point-to-multipoint Multiprotocol Label Switching Traffic Engineering (MPLS-TE) definitions.

CISCO-IETF-PPVPN-MPLS-VPN-MIB

The CISCO-IETF-PPVPN-MPLS-VPN-MIB is an extension of the MPLS-VPN-MIB. It contains a new notification, mplsNumVrfRouteMaxThreshCleared, which was added with MPLS-VPN-MIB-DRAFT-05.

CISCO-IETF-PW-ATM-MIB

The CISCO-IETF-PW-ATM-MIB contains managed object definitions for pseudowire (PW) emulation of ATM over packet-switched networks (PSNs).

MIB Constraints

Table 3-36 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-IETF-PW-ATM-MIB.

Table 3-36 CISCO-IETF-PW-ATM-MIB Constraints

MIB Object	Notes
CpwVcAtmPerfEntry	
• cpwAtmCellsReceived	Not supported, returns zero.
• cpwAtmCellsSent	Not supported, returns zero.
• cpwAtmCellsRejected	Not supported, returns zero.
• cpwAtmCellsTagged	Not supported, returns zero.
• cpwAtmHCCellsReceived	Not supported, returns zero.
• cpwAtmHCCellsRejected	Not supported, returns zero.
• cpwAtmHCCellsTagged	Not supported, returns zero.
• cpwAtmAvgCellsPacked	Not supported, returns zero.

CISCO-IETF-PW-ENET-MIB

The CISCO-IETF-PW-ENET-MIB contains objects that describe the model for managing Ethernet point-to-point pseudowire services over a packet-switched network (PSN).

MIB Constraints

Table 3-37 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-IETF-PW-ENET-MIB.

Table 3-37 CISCO-IETF-PW-ENET-MIB Constraints

MIB Object	Notes
cpwVcEnetMplsPriMappingTable	Not supported.
cpwVcEnetStatsTable	Not supported.

CISCO-IETF-PW-MIB

The CISCO-IETF-PW-MIB contains managed object definitions for pseudowire (PW) operations.

MIB Constraints

Table 3-38 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-IETF-PW-MIB.

Table 3-38 CISCO-IETF-PW-MIB Constraints

MIB Object	Notes
cpwVcTable	
• CpwVcEntry	Not-accessible.
• cpwVcIndex	Not-accessible.
• cpwVcType	Read-only.
• cpwVcOwner	Read-only.
• cpwVcPsnType	Read-only.
• cpwVcSetUpPriority	Not implemented.
• cpwVcHoldingPriority	Not implemented.
• cpwVcInboundMode	Read-only.
• cpwVcPeerAddrType	Read-only.
• cpwVcPeerAddr	Read-only.
• cpwVcID	Read-only.
• cpwVcLocalGroupID	Read-only.
• cpwVcControlWord	Read-only.
• cpwVcLocalIfMtu	Read-only.
• cpwVcLocalIfString	Read-only.
• cpwVcRemoteControlWord	Read-only.
• cpwVcOutboundVcLabel	Read-only.
• cpwVcInboundVcLabel	Read-only.
• cpwVcName	Read-only.
• cpwVcDescr	Read-only.
• cpwVcAdminStatus	Read-only.

Table 3-38 CISCO-IETF-PW-MIB Constraints

MIB Object	Notes
• cpwVcTimeElapsed	Not implemented.
• cpwVcRowStatus	Read-only.
• cpwVcStorageType	Read-only.
cpwVcPerfCurrentTable	
• cpwVcPerfCurrentEntry	Not implemented.
• cpwVcPerfCurrentInHCPackets	Not implemented.
• cpwVcPerfCurrentInHCBytes	Not implemented.
• cpwVcPerfCurrentOutHCBytes	Not implemented.
• cpwVcPerfCurrentOutHCPackets	Not implemented.
cpwVcPerfIntervalTable	
• cpwVcPerfIntervalEntry	Not implemented.
• cpwVcPerfIntervalNumber	Not implemented.
• cpwVcPerfIntervalValidData	Not implemented.
• cpwVcPerfIntervalInHCPackets	Not implemented.
• cpwVcPerfIntervalInHCBytes	Not implemented.
• cpwVcPerfIntervalOutHCPackets	Not implemented.
• cpwVcPerfIntervalOutHCBytes	Not implemented.
cpwVcNotifRate	Not implemented.

CISCO-IETF-PW-MPLS-MIB

The CISCO-IETF-PW-MPLS-MIB contains objects that complement the CISCO-IETF-PW-MIB for PW operation over MPLS.

MIB Constraints

Table 3-39 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-IETF-PW-MPLS-MIB.

Table 3-39 CISCO-IETF-PW-MPLS-MIB Constraints

MIB Object	Notes
cpwVcMplsOutboundIndexNext	Not supported.
cpwVcMplsInboundIndexNext	Not supported.

CISCO-IETF-PW-TDM-MIB

The CISCO-IETF-PW-TDM-MIB contains managed object definitions for encapsulating TDM (T1,E1, T3, E3, NxDS0) as pseudowires over packet-switching networks (PSNs).

CISCO-IF-EXTENSION-MIB

The CISCO-IF-EXTENSION-MIB contains objects that provide additional interface-related information that is not available in the IF-MIB (RFC 2863).

MIB Constraints

Table 3-40 lists constraints that the Cisco ASR 903 Series Router places on the object in the CISCO-IF-EXTENSION-MIB

Table 3-40 CISCO-IF-EXTENSION-MIB Constraints

MIB Object	Notes
cieIfInterfaceTable	
• cieIfDhcpMode	Not implemented.
• cieIfMtu	Not implemented.
• cieIfContextName	Not implemented.
• cieIfKeepAliveEnabled	Not supported for ATM interfaces.
cieSystemMtu	Not implemented.
cieIfUtilTable	Not supported for GE interfaces.
cieIfDot1dBaseMappingTable	Not implemented.
cieIfDot1qCustomEtherTypeTable	Not implemented.
cieIfNameMappingTable	Not implemented.

Notes

Some objects defined in cieIfPacketStatsTable and cieIfInterfaceTable are applicable only to physical interfaces. As a result, this table may be sparse for non-physical interfaces.

ATM interfaces do not support the cieIfKeepAliveEnabled object.

CISCO-IGMP-FILTER-MIB

The CISCO_IGMP-FILTER-MIB provides a mechanism for users to configure the system to intercept Internet Group Management Protocol (IGMP) joins for IP Multicast groups identified in this MIB and only allow certain ports to join certain multicast groups.

CISCO-IMAGE-MIB

The CISCO-IMAGE-MIB contains objects that identify the capabilities and characteristics of the Cisco IOS XE image.

CISCO-IMAGE-LICENSE-MGMT-MIB

The CISCO-IMAGE-LICENSE-MGMT-MIB contains objects to manage the running image level of a Cisco device. The licensing mechanism provides flexibility to run a device on a chosen image level. This mechanism is referred to as image level licensing. Image level licensing leverages the universal image-based licensing solution.

CISCO-IP-STAT-MIB

The CISCO-IP-STAT-MIB contains objects to manage the collection and display of IP statistics, categorized by IP precedence and the MAC address associated with IP packets. To use the MIB to access additional IP statistics, the **ip accounting mac-address** and **ip accounting precedence** commands must be issued at the CLI.

CISCO-IPMROUTE-MIB

The CISCO-IPMROUTE-MIB contains objects to manage IP multicast routing on the router.

CISCO-IPSLA-ETHERNET-MIB

The CISCO-IPSLA-ETHERNET-MIB contains objects to manage IP SLA Auto-Ethernet-CFM operations and Ethernet Jitter statistics. IP SLA is a capability that utilizes active monitoring for network performance. It can be used for network troubleshooting, network assessment, and health monitoring. Ethernet Jitter is used to measure metrics, such as round-trip time (RTT), Jitter, frame loss, and one-way latency by sending multiple enhanced CFM frames at specified interval to a particular Maintenance End Point (MEP).

CISCO-LAG-MIB

The CISCO-LAG-MIB contains objects to manage link aggregation (LAG) on the router, as defined by IEEE Standard 802.3ad. The MIB contains link aggregation information that supplements to IEEE8023-LAG-MIB or is specific to Cisco products.

CISCO-L2-CONTROL-MIB

The CISCO-L2-CONTROL-MIB contains objects that provide a control feature for devices with Layer 2 functions, such as the VLAN MAC limit control.

CISCO-LICENSE-MGMT-MIB

The CISCO-LICENSE-MGMT-MIB contains objects to manage the licenses on the system. The licensing mechanism provides flexibility to enforce licensing for various features in the system.

CISCO-MAC-NOTIFICATION-MIB

The CISCO-MAC-NOTIFICATION-MIB is for configuration of the MAC notification feature. MAC notification is a mechanism to inform monitoring devices when there are MAC addresses learned or removed from the forwarding database of the monitored devices.

CISCO-MEMORY-POOL-MIB

The CISCO-MEMORY-POOL-MIB contains objects that represents the different types of memory pools that are present in a managed device. Memory pools are categorized into two groups:

- Predefined pools
- Dynamic pools

CISCO-MPLS-LSR-EXT-STD-MIB

The CISCO-MPLS-LSR-EXT-STD-MIB contains generic object definitions for MPLS Label Switching Router (LSR) in transport networks.

MIB Constraints

Table 3-41 lists the constraints that the router places on the objects in the CISCO-MPLS-LSR-EXT-STD-MIB.

Table 3-41 CISCO-MPLS-LSR-EXT-STD-MIB Constraints

MIB Object	Notes
cmplsLsrExtObjects	Read-only.
cmplsTunnelOppositeDirPtr	Not implemented.

CISCO-MPLS-TC-EXT-STD-MIB

The CISCO-MPLS-TC-EXT-STD-MIB contains textual conventions for MPLS based transport networks.

MIB Constraints

Table 3-41 lists the constraints that the router places on the objects in the CISCO-MPLS-TC-EXT-STD-MIB.

Table 3-42 CISCO-MPLS-TC-EXT-STD-MIB Constraints

MIB Object	Notes
cmplsTeExtObjects	Read-only.

CISCO-MVPN-MIB

The CISCO-MVPN-MIB contains managed object definitions for the Cisco implementation of multicast in VPNs defined by the Internet draft, draft-rosen-vpn-mcast-05.txt.

The Multicast VPN MIB feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring of a Multicast VPN (MVPN). Using the MVPN MIB, network administrators can access MVRF information from PE routers. This information can be accessed for VPN traffic across multiple CE sites in real time. SNMP operations can be performed to monitor the MVRFs on the PE routers, using the get and set commands. These commands are entered on the Network management system (NMS) workstation for which the SNMP has been implemented. The NMS workstations is also known as the SNMP manager.

Note Currently only IPv4 is supported.

Note For all MIB objects with "read-create" access privileges, currently only "read-only" access is supported.

For more information on this MIB, please access the following link:
https://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/mcvpnmib.html

CISCO-NETSYNC-MIB

The CISCO-NETSYNC-MIB contains objects to monitor network synchronization based on ITU-T G.781 clock selection.

CISCO-NHRP-EXT-MIB

The CISCO-NHRP-EXT-MIB module is an extension of the NHRP MIB. It defines notifications associated with critical events in the Next Hop Resolution Protocol (NHRP) as defined in RFC 2332.

CISCO-NTP-MIB

The CISCO-NTP-MIB contains objects to monitor a Network Time Protocol (NTP) server. NTP is used to synchronize timekeeping among a set of distributed time servers and clients. Primary time servers, which are synchronized to national time standards, are connected to widely accessible resources such as backbone gateways. These primary servers send timekeeping information to other time servers, and perform clock checking to eliminate timekeeping errors due to equipment or propagation failures.

CISCO-OSPF-MIB

The CISCO-OSPF-MIB contains objects for managing OSPF implementation. Most of the MIB definitions are based on the IETF draft draft-ietf-ospf-mib-update-05.txt and include support for OSPF sham link. The CISCO-OSPF-MIB is an extension to the OSPF-MIB defined in RFC 1850.

CISCO-OSPF-TRAP-MIB

The CISCO-OSPF-TRAP-MIB contains new and modified notification objects and events, which are defined in the latest version of the OSPF-MIB IETF (draft draftietf-ospf-mib-update-05.txt) in addition to support for the OSPF sham link.

CISCO-PIM-MIB

The CISCO-PIM-MIB defines Cisco-specific objects and variables for managing Protocol Independent Multicasts (PIMs) on the router. These MIB definitions are an extension of those in RFC 2934, which is the IETF PIM MIB.

CISCO-PING-MIB

The CISCO-PING-MIB contains objects to manage ping requests on the router.

CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB displays memory and CPU usage on the router and describes active system processes. CPU utilization presents a status of how busy the system is. The numbers are a ratio of the current idle time over the longest idle time. (This information should be used only as an estimate.)

MIB Constraints

Table 3-43 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-PROCESS-MIB.

Table 3-43 CISCO-PROCESS-MIB Constraints

MIB Object	Notes
cpmProcessTable	
• cpmProcExtPriority	Read-only.
cpmCPURisingThreshold	Not supported.
cpmCPUFallingThreshold	Not supported.

Note The cpmCPUTotalTable object contains only one entry for RSP CPUs.

CISCO-PROCESS-MIB Usage

The cpmCPUTotal5sec, cpmCPUTotal1min, and cpmCPUTotal5min objects have been deprecated and replaced by cpmCPUTotal5secRev, cpmCPUTotal1minRev, and cpmCPUTotal5minRev, respectively.

Note When an object is deprecated, it does not mean that an object instance may not be returned. For these deprecated objects, object instances are returned. However, their returned values must be ignored. The values returned by the new objects must be used.

Note The CPU utilization objects, such as cpmCPUTotal5sec, cpmCPUTotal1min, and cpmCPUTotal5min are calculated for all the processes used by the CPU except under idle condition.

Note For the Cisco ASR 903 Series Router, there are no separate FPs.

Table 3-44 lists the support matrix for the CISCO-PROCESS-MIB cpmCPUTotalTable object.

Table 3-44 Support-Matrix for cpmCPUTotalTable

cpmCPUTotalTable Objects	RSP CPU	Stdby RSP CPU
cpmCPULoadAvg1min	Yes	No
cpmCPULoadAvg5min	Yes	No
cpmCPULoadAvg15min	Yes	No
cpmCPUMemoryCommitted	Yes	No
cpmCPUTotalPhysicalIndex	Yes	No
cpmCPUTotal5sec	Yes	No
cpmCPUTotal1min	Yes	No
cpmCPUTotal5min	Yes	No
cpmCPUTotal5secRev	Yes	No
cpmCPUTotal1minRev	Yes	No
cpmCPUTotal5minRev	Yes	No
cpmCPUMonInterval	No	No
cpmCPUTotalMonIntervalValue	No	No
cpmCPUInterruptMonIntervalValue	No	No
cpmCPUMemoryUsed	Yes	No
cpmCPUMemoryFree	Yes	No
cpmCPUMemoryKernelReserved	No	No
cpmCPUMemoryLowest	Yes	No

Table 3-45 lists the support matrix for the CISCO-PROCESS-MIB cpmProcessTable and cpmProcessExtRevTable objects for RSP CPU.

Table 3-45 Support-Matrix for cpmProcessTable and cpmProcessExtRevTable for RSP CPU

cpmProcessTable and cpmProcessRevExtTable Objects	IOSD Process [Process Name: ppc_linux_iosd-]	Other Process [Process Name: Cmand, hman, iomd]
cpmProcessName	Yes	Yes
cpmProcessuSecs	No	No
cpmProcessTimeCreated	Yes	Yes
cpmProcessAverageUSecs	Yes	Yes
cpmProcExtMemAllocatedRev	Yes	Yes
cpmProcExtMemFreedRev	No	No
cpmProcExtInvokedRev	No	No
cpmProcExtRuntimeRev	No	No
cpmProcExtUtil5SecRev	No	No
cpmProcExtUtil1MinRev	No	No
cpmProcExtUtil5MinRev	No	No
cpmProcExtPriorityRev	Yes	Yes
cpmProcessType	No	No
cpmProcessRespawn	No	No
cpmProcessRespawnCount	No	No
cpmProcessRespawnAfterLastPatch	No	No
cpmProcessMemoryCore	No	No
cpmProcessLastRestartUser	No	No
cpmProcessTextSegmentSize	No	No
cpmProcessDataSegmentSize	No	No
cpmProcessStackSize	No	No
cpmProcessDynamicMemorySize	No	No

Table 3-46 lists the support matrix for the CISCO-PROCESS-MIB cpmVirtualProcessTable object.

Table 3-46 Support-matrix for cpmVirtualProcessTable

cpmVirtualProcessTable Objects	Process running under Active RSP IOSD Process
cpmVirtualProcessName	Yes
cpmVirtualProcessUtil5Sec	Yes
cpmVirtualProcessUtil1Min	Yes
cpmVirtualProcessUtil5Min	Yes
cpmVirtualProcessMemAllocated	Yes
cpmVirtualProcessMemFreed	Yes

Table 3-46 Support-matrix for cpmVirtualProcessTable (continued)

cpmVirtualProcessTable Objects	Process running under Active RSP IOSD Process
cpmVirtualProcessInvokeCount	Yes
cpmVirtualProcessRuntime	Yes

CISCO-PRODUCTS-MIB

The CISCO-PRODUCTS-MIB lists the object identifiers (OIDs) assigned to the Cisco hardware platforms.

CISCO-PTP-MIB

The CISCO-PTP-MIB supports the Precision Timing Protocol (PTP) feature on Cisco devices. The protocol enables heterogeneous systems that include clocks of various inherent precision, resolution, and stability to synchronize to a grandmaster clock.

CISCO-RF-MIB

The CISCO-RF-MIB provides configuration control and status information for the redundancy framework subsystem. The redundancy framework subsystem provides a mechanism for logical redundancy of the software functionality and is designed to support 1:1 redundancy for the processor cards.

CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB

The CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB defines objects required for managing Resilient Ethernet Protocol (REP). REP is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP). REP provides the functionality to control network loops, handle link failures, and improve convergence time.

CISCO-RTTMON-ICMP-MIB

The CISCO-RTTMON-ICMP-MIB is an extension to the CISCO-RTTMON-MIB for ICMP operations. The ICMP Jitter operation provides capability to measure metrics, such as RTT, Jitter, packet loss, and one-way latency by sending ICMP timestamp streams to destination devices.

CISCO-RTTMON-IP-EXT-MIB

The CISCO-RTTMON-IP-EXT-MIB provides extensions for the tables in CISCO-RTTMON-MIB to support IP layer extensions, specifically IPv6 addresses and other information related to IPv6 standards.

CISCO-RTTMON-MIB

The CISCO-RTTMON-MIB contains objects to monitor network performance. The MIB provides information about the response times of network resources and applications. Each conceptual round-trip time (RTT) control row in the MIB represents a single probe, which is used to determine an entity's response time. The probe defines an RTT operation to perform (for example, an FTP or HTTP get request), and the results indicate whether the operation succeeded or failed, and how long it took to complete.

If you plan to schedule an RTT operation, see Table 3-47 for information about rttMonScheduleAdminRttStartTime in the rttMonScheduleAdminTable.

Note An rttMonCtrlOperConnectionLostOccurred trap is generated when an RTT connection cannot be established to the destination router because the router responder application is not running. However, the trap is not generated if the physical connection to the router is lost.

MIB Constraints

Table 3-47 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-RTTMON-MIB.

Table 3-47 CISCO-RTTMON-MIB Constraints

MIB Object	Notes
RttMonProtocol	The following values are not supported: • snaRUEcho • snaLU0EchoAppl
rttMonApplAuthTable	Not supported.
rttMonCtrlAdminTable • rttMonCtrlAdminRttType	Supported values are: • echo(1) • pathEcho(2) • udpEcho(5) • tcpConnect(6) • http(7) • dns(8) • jitter(9) • ftp(12) All other values not supported.
rttMonEchoAdminTable • rttMonEchoAdminProtocol	Supported values: • ipIcmpEcho(2) • ipUdpEchoAppl(3) • ipTcpConn(24) • httpAppl(25) • dnsAppl(26) • jitterAppl(27) • ftpAppl(30) All other values not supported.
rttMonScheduleAdminTable • rttMonScheduleAdminRttStartTime	Before setting this object to a date/time value, make sure the ESR clock was set through the CLI **clock set** command. Otherwise, the scheduled RTT operation does not run.
rttMonHistoryCollectionTable	HTTP and Jitter types are not supported.

CISCO-RTTMON-RTP-MIB

The CISCO-RTTMON-RTP-MIB is an extension to the CISCO-RTTMON-MIB for Cisco IP SLA Real-Time Transport Protocol (RTP) operation. This operation provides the capability to measure voice quality metrics, such as RTT, Jitter, and Mean Opinion Score (MOS) by setting up RTP stream between two routers. In voice communications, particularly Internet telephony, MOS provides a numerical measure of the quality of human speech at the destination end of the circuit.

CISCO-SNMP-TARGET-EXT-MIB

The CISCO-SNMP-TARGET-EXT-MIB is an extension of the SNMP-TARGET-MIB specified in RFC2273.

CISCO-STP-EXTENSIONS-MIB

The CISCO-STP-EXTENSIONS-MIB contains objects to manage the Cisco extensions to the IEEE 802.1D Spanning Tree Protocol (STP).

Note For the CISCO-STP-EXTENSIONS-MIB, only the traps and notification for the stpxRootInconsistency object have been verified.

CISCO-SONET-MIB

The CISCO-SONET-MIB contains objects to describe SONET/SDH interfaces on the router. This MIB is an extension of the standard SONET-MIB (RFC 2558). The CISCO-SONET-MIB has objects that provide additional SONET-related information, which is not found in the SONET-MIB.

Note CISCO-SONET-MIB supports SONET traps that are seen when the line, section, path status changes, and notifications are enabled.

MIB Constraints

Table 3-48 describes the constraints that the Cisco ASR 903 Series Router places on the objects in the CISCO-SONET-MIB.

Table 3-48 CISCO-SONET-MIB Constraints

MIB Object	Notes
csConfigTable	Not implemented.
csVTConfigTable	Not implemented.
csAPSConfigTable	Not implemented.
cssTraceTable	Not implemented.

Table 3-48 CISCO-SONET-MIB Constraints (continued)

MIB Object	Notes
cspTraceTable	Not implemented.
csStatsTable	Not implemented.
cspConfigTable	Not implemented.

Note Only the section, line, and path totals objects from the ciscoSonetStatsMIBGroup and the complete ciscoSonetEnableGroup is supported. All network elements containing one or more SONET interfaces should implement this MIB.

CISCO-SYSLOG-MIB

The CISCO-SYSLOG-MIB contains all system log messages generated by the Cisco IOS XE software. The MIB provides a way to access these system log messages through the SNMP. All Cisco IOS XE system log messages contain the message name and its severity, message text, the name of the entity generating the message, and an optional time stamp. The MIB also contains a history of system log messages and counts related to system log messages.

Note The Cisco ASR 903 Series Router can be configured to send system log messages to a system log server.

Note The MIB does not keep track of messages generated from debug commands entered through the CLI.

CISCO-TCP-MIB

The CISCO-TCP-MIB contains objects to manage the TCP on the router. This MIB is an extension to the IETF TCP MIB.

CISCO-VRF-MIB

The CISCO-VRF-MIB contains objects to manage and provision the network virtualization features. Virtual Routing and Forwarding (VRF) is an extension of IP routing that provides multiple routing instances.

DS1-MIB (RFC 2495)

The DS1-MIB(RFC-2495) contains a description of the DS1, E1, DS2, and E2 interface objects.

MIB Constraints

Table 3-49 describes the constraints that the Cisco ASR 903 Series Router places on the objects in the DS1-MIB. For detailed definitions of the MIB objects, see the corresponding MIB.

Table 3-49 DS1-MIB Constraints

MIB Object	Notes
dsx1ConfigTable	
• dsx1LineStatusChangeTrapEnable	Read-only. This MIB object cannot be set through SNMP. The **snmp-server enable traps ds1** command can be used to enable status change traps.
• dsx1Channelization	Read-only.
• dsx1LineLength	Read-only.
• dsx1LineType	Read-only.
• dsx1LineCoding	Read-only.
• dsx1SendCode	Read-only.
• dsx1CircuitIdentifier	Read-only.
• dsx1LoopbackConfig	Read-only.
• dsx1SignalMode	Read-only.
• dsx1TransmitClockSource	Read-only.
• dsx1Fdl	Read-only.
• dsx1LoopbackStatus	Payload loopbacks are not supported (dsx1NearEndPayloadLoopback, dsx1FarEndPayloadLoopback).
dsx1FracTable	Not implemented.
dsx1FarEndIntervalTable	Not implemented.

ENTITY-MIB (RFC 4133)

The ENTITY-MIB (RFC 4133) allows functional component discovery. It is used to represent physical and logical entities (components) in the router and manages those entities. The current software release supports the RFC 4133 version of this MIB.

The following are the conformance groups contained in the ENTITY-MIB:

- entityPhysical group—Describes the physical entities managed by a single agent.
- entityLogical group—Describes the logical entities managed by a single agent.
- entityMapping group—Describes the associations between the physical entities, logical entities, interfaces, and non-interface ports managed by a single agent.
- entityGeneral group—Describes general system attributes shared by potentially all types of entities managed by a single agent.
- entityNotifications group—Contains status indication notifications.

The following groups are added from RFC 4133:

- entityPhysical2 group—This group augments the entityPhysical group.
- entityLogical2 group—Describes the logical entities managed by a single agent, and replaces entityLogical group.

The MIB table entPhysicalTable identifies the physical entities in the router. The entPhysicalTable contains a single row for the Cisco ASR 903 Series Router chassis and a row for each entity in the chassis. A physical entity may contain other entities. For example, an IM in IM Bay 0 with one A900-IMA8T-CU-IM in subslot 0/1 supports the following entities in this SNMP. Output for IMs, sensors on the subslot, and IM ports:

```
entPhysicalDescr.550 = 8-port Gigabit Ethernet Interface Module
entPhysicalContainedIn.550 = 5
entPhysicalDescr.551 = A900-IM8T
entPhysicalContainedIn.551 = 550
entPhysicalDescr.552 = A900-IM8T
entPhysicalContainedIn.552 = 550
entPhysicalDescr.553 = A900-IM8T
entPhysicalContainedIn.553 = 550
entPhysicalDescr.554 = A900-IM8T
entPhysicalContainedIn.554 = 550
entPhysicalDescr.555 = A900-IM8T
entPhysicalContainedIn.555 = 550
entPhysicalDescr.556 = A900-IM8T
entPhysicalContainedIn.556 = 550
entPhysicalDescr.557 = A900-IM8T
entPhysicalContainedIn.557 = 550
entPhysicalDescr.558 = A900-IM8T
entPhysicalContainedIn.558 = 550
entPhysicalDescr.567 = subslot 0/1 temperature Sensor 0
entPhysicalContainedIn.567 = 550
entPhysicalDescr.568 = subslot 0/1 temperature Sensor 1
entPhysicalContainedIn.568 = 550
entPhysicalDescr.569 = subslot 0/1 temperature Sensor 2
entPhysicalContainedIn.569 = 550
entPhysicalDescr.570 = subslot 0/1 temperature Sensor 3
entPhysicalContainedIn.570 = 550
entPhysicalDescr.571 = subslot 0/1 temperature Sensor 4
entPhysicalContainedIn.571 = 550
entPhysicalDescr.579 = subslot 0/1 voltage Sensor 0
entPhysicalContainedIn.579 = 550
entPhysicalDescr.580 = subslot 0/1 voltage Sensor 1
entPhysicalContainedIn.580 = 550
entPhysicalDescr.581 = subslot 0/1 voltage Sensor 2
entPhysicalContainedIn.581 = 550
entPhysicalDescr.582 = subslot 0/1 voltage Sensor 3
entPhysicalContainedIn.582 = 550
entPhysicalDescr.583 = subslot 0/1 voltage Sensor 4
entPhysicalContainedIn.583 = 550
entPhysicalDescr.584 = subslot 0/1 voltage Sensor 5
entPhysicalContainedIn.584 = 550
entPhysicalDescr.800 = 16 port T1/E1 IM
```

Note The IM A900-IMA4OS has only four ports modelled.

For more information on the ENTITY-MIB, refer Appendix A, “CISCO-ENTITY-ALARM-MIB.”

For the Cisco ASR 903 Series Router platform, the entPhysicalParentRelPos values are populated with the slot numbers (except for the RP, and PEM slot numbers) provided in the external label.

Table 3-50 lists the mapping between external labels and entPhysicalParentRelPos values.

Table 3-50 Mapping the External Labels to the entPhysicalParentRelPos Values

Type	External Label	Value
IM Bay	0 to 5	0 to 5 match the external label.
RSP Container	R0 and R1	6 for R0, and 7 for R1.
Power Supply Bay	0 and 1	11 for PEM 0 and 12 for PEM 1.
FanTray Bay	__	13

Table 3-51 lists the values of the affected MIB table objects in the Cisco ASR 903 Series Router:

Table 3-51 Affected MIB Objects in a Cisco ASR 903 Series Router

Type	External Label	Value
entPhysicalContainedIn	RSP Slot	entPhysicalIndex of Chassis.
	RSP Module	entPhysicalIndex of RSP Slot.
	IM Bay	entPhysicalIndex of Chassis.
	IM	entPhysicalIndex of IM Bay.
	Power Supply Bay	entPhysicalIndex of Chassis.
	FanTray Bay	entPhysicalIndex of Chassis.

Table 3-52 lists the fans supported on a Cisco ASR 903 Series Router.

Table 3-52 Fans Supported on a Cisco ASR 903 Series Router

Module	Number of Fans
ASR 903 FAN Tray	12

MIB Constraints

Table 3-53 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the ENTITY-MIB.

Table 3-53 ENTITY-MIB Constraints

MIB Object	Notes
entPhysicalSoftwareRev	Supported for RSP module.
entPhysicalAssetAlias	Not supported.
entPhysicalAssetId	Not supported for transceiver modules and USBs. Implemented only as read-write for the following entPhysicalClass entities: • Chassis • Powersupply • Module
entPhysicalHardwareRev	Not implemented for USB.
entPhysicalSerialNum	Implemented as read-only. Not implemented for USB.
entPhysicalModelName	Not implemented for USB.
entPhysicalMfgName	Not implemented for USB.
entPhysicalUris	Not implemented for USB. Implemented as read-only.
entPhysicalAlias	Not supported for transceiver modules and USB . Implemented only as read-write for the following entPhysicalClass entities: • Chassis • Powersupply • Module
entPhysicalMfgDate	Not implemented.

Note When both primary and secondary RSPs are up and running, entities for standby USB flash and boot flash are not populated for the ENTITY-MIB.

Note For cevModuleASR903UnknownRSP object, only the RSP module entry is populated without any child entities.

ENTITY-SENSOR-MIB (RFC 3433)

The ENTITY-SENSOR-MIB (RFC 3433) contains objects that manage physical sensors, which are represented in the Entity-MIB with entPhysicalEntry and an entPhysicalClass value of sensor(8). The ENTITY-SENSOR-MIB contains a single table called the entPhySensorTable.

Note These sensors are supported on the CISCO-ENTITY-SENSOR-MIB. Unit tests can be performed to ensure that all the sensors are modelled in the MIB.

ENTITY-STATE-MIB

The ENTITY-STATE-MIB defines objects to extend the functionality provided by the ENTITY-MIB. This MIB supports the entities having these entPhysicalClass values:

- Chassis
- Container (RSP slot, IM bay, PS bay and Fan-tray bay)
- Module (RSP, IM, and transceiver)
- PowerSupply
- Fan

MIB Constraints

Table 3-54 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the ENTITY-STATE-MIB.

Table 3-54 ENTITY-STATE-MIB Constraints

MIB Object	Notes
entStateAlarm	Valid values are: • critical • major • minor • warning These values indicate the CISCO-ENTITY-ALARM-MIB alarm types.
entStateAdmin	Read-only.

Note Power supply and fan alarms are generated on either the Power Entry Module or FanTray module. Therefore, no alarm is generated on the entStateAlarm object associated with either the power supply or the fan.

ETHER-WIS (RFC 3637)

The ETHER-WIS (RFC 3637) MIB contains objects to manage application details for the Ethernet WAN Interface Sublayer (WIS).

MIB Constraints

Table 3-55 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the ETHER-WIS (RFC 3637) MIB.

Table 3-55 ETHER-WIS (RFC 3637) MIB Constraints

MIB Object	Note
etherWisDeviceTable	Not supported.
etherWisSectionCurrentTable	Not supported.
etherWisFarEndPathCurrentTable	Not supported.

Note WAN-PHY is not fully compliant with the SONET/SDH optical and electrical specifications.

Note SONET layer is not modelled for the Ethernet WIS port.

ETHERLIKE-MIB (RFC 3635)

The ETHERLIKE-MIB contains objects to manage Ethernet-like interfaces.

MIB Constraints

Table 3-56 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the ETHERLIKE-MIB. Any objects not listed in a table are implemented as defined in the MIB.

Table 3-56 ETHERLIKE-MIB Constraints

MIB Object	Notes
dot3CollTable	Not implemented.
dot3ControlTable	Not implemented.
dot3Control	Not implemented.
dot3PauseAdminMode	Read-only.

EVENT-MIB (RFC 2981)

The EVENT-MIB (RFC 2981) contains objects to define event triggers and actions for network management purposes.

EXPRESSION-MIB

The EXPRESSION-MIB (RFC 2982) contains objects to define the expressions of MIB objects for network management purposes.

HC-ALARM-MIB

The HC-ALARM-MIB defines Remote Monitoring MIB extensions for High Capacity Alarms.

MIB Tables

Table 3-57 lists the tables in HC-ALARM-MIB.

Table 3-57 HC-ALARM-MIBTables

MIB Table	Description
hcAlarmTable	A list of entries for the configuration of high capacity alarms.

HC-RMON-MIB

The HC-RMON- MIB augments the original RMON MIB as specified in RFC 1757 and RFC 1513, and RMON2 MIB as specified in RFC 2021. It manages the remote monitoring device implementations.

IEEE8021-CFM-MIB

The IEEE8021-CFM-MIB is a Connectivity Fault Management (CFM) module for managing IEEE 802.1ag.

MIB Constraints

Table 3-56 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the IEEE8021-CFM-MIB.

Table 3-58 IEEE8021-CFM-MIB Constraints

MIB Object	Notes
dot1agCfmMepTransmitLbmStatus	Not supported.
dot1agCfmMepTransmitLbmDestMacAddress	Not supported.
dot1agCfmMepTransmitLbmDestMepId	Not supported.
dot1agCfmMepTransmitLbmDestIsMepId	Not supported.
dot1agCfmMepTransmitLbmMessages	Not supported.
dot1agCfmMepTransmitLbmDataTlv	Not supported.

Table 3-58 IEEE8021-CFM-MIB Constraints (continued)

MIB Object	Notes
dot1agCfmMepTransmitLbmVlanPriority	Not supported.
dot1agCfmMepTransmitLbmVlanDropEnable	Not supported.
dot1agCfmMepTransmitLbmResultOK	Not supported.
dot1agCfmMepTransmitLbmSeqNumber	Not supported.
dot1agCfmMepTransmitLtmStatus	Not supported.
dot1agCfmMepTransmitLtmFlags	Not supported.
dot1agCfmMepTransmitLtmTargetMacAddress	Not supported.
dot1agCfmMepTransmitLtmTargetMepId	Not supported.
dot1agCfmMepTransmitLtmTargetIsMepId	Not supported.
dot1agCfmMepTransmitLtmTtl	Not supported.
dot1agCfmMepTransmitLtmResult	Not supported.
dot1agCfmMepTransmitLtmSeqNumber	Not supported.
dot1agCfmMepTransmitLtmEgressIdentifier	Not supported.

Note The IEEE8021-CFM-MIB does not support SET operation.

IEEE8021-CFM-V2-MIB

The IEEE8021-CFM-V2-MIB is a Connectivity Fault Management (CFM) version 2 module for managing IEEE 802.1ag.

Note The IEEE8021-CFM-V2-MIB does not support SET operation.

IEEE8023-LAG-MIB

The IEEE 8023-LAG-MIB is the Link Aggregation module for managing IEEE Std 802.3ad.

IF-MIB (RFC 2863)

The IF-MIB (RFC 2863) describes the attributes of physical and logical interfaces (network interface sublayers). The router supports the ifGeneralGroup of MIB objects for all layers (ifIndex, ifDescr, ifType, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, ifLastChange, ifName, ifLinkUpDownTrapEnable, ifHighSpeed, and ifConnectorPresent).

One of the most commonly used identifiers in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface.

Note The ifInDiscards, ifInErrors, ifInUnknownProtos, ifOutDiscards, and ifOutErrors IF-MIB objects are not supported for Gigabit subinterfaces.

Note The IF-MIB supports these modes for A900-IMA4OS:
- Channel-group under c-11 mode in au-3
- Channel-group under c-12 mode in au-4
- CEM under c-12 mode in au-4
- CEM under c-11 mode in au-3

Note BDI interfaces are not supported for IF-MIB as the counter values are not updated for this MIB.

Layering for A900-IMA4OS

On querying the ifStackStatus object, the CEM interface and the Channel group show the layers as illustrated in Figure 3-1 and Figure 3-2.

Figure 3-1 Layering Shown by the CEM Interface

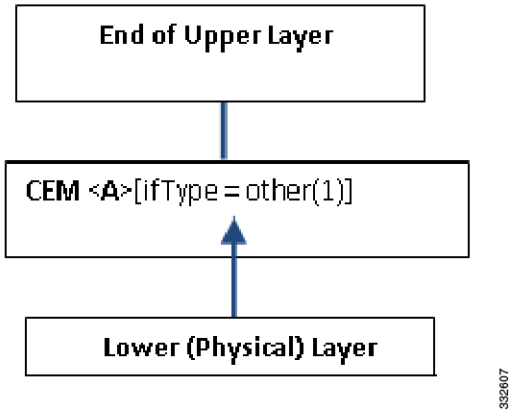
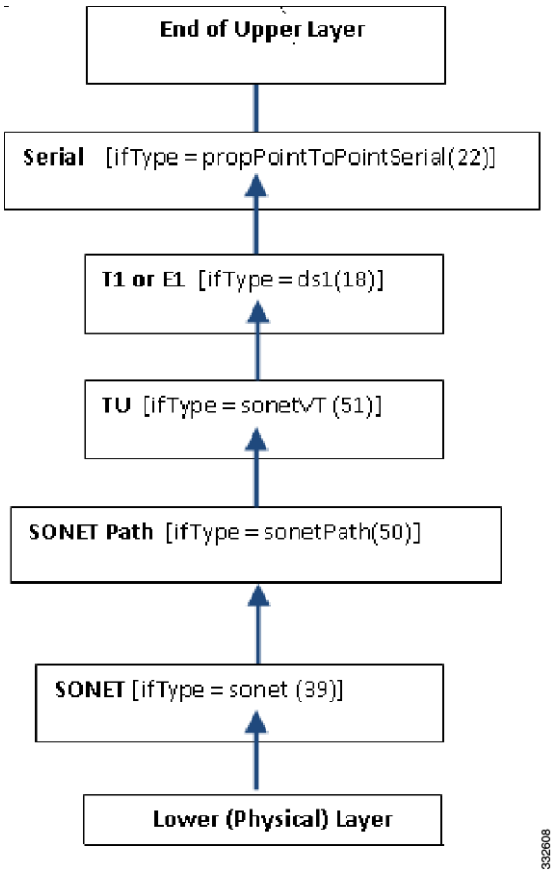


Figure 3-2 Layering Shown by the Channel Group



MIB Constraints

Table 3-59 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the IF-MIB.

Table 3-59 IF-MIB Constraints

MIB Object	Notes
ifOutErrors	Not supported for ATM subinterfaces.
ifPromiscuousMode	Read-only.
ifStackStatus	Read-only.

IGMP-STD-MIB (RFC 2933)

The IGMP-STD-MIB(RFC 2933) manages Internet Group Management Protocol (IGMP).

INT-SERV-GUARANTEED-MIB

The INT-SERV-GUARANTEED-MIB describes the guaranteed service of the Integrated Services Protocol.

INTEGRATED-SERVICES-MIB

The INTEGRATED-SERVICES-MIB contains objects to manage the Integrated Services Protocol.

IP-FORWARD-MIB (RFC 4292)

The IP-FORWARD-MIB (RFC 4292) contains objects to control the display of classless interdomain routing (CIDR) multipath IP Routes.

IP-MIB (RFC 4293)

The IP-MIB (RFC 4293) module contains objects for managing IP and Internet Control Message Protocol (ICMP) implementations, but not their management of IP routes.

MIB Constraints

Table 3-60 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the IP-MIB.

Table 3-60 IP-MIB Constraints

MIB Object	Notes
ipv4InterfaceTableLastChange	Not implemented.
ipv4InterfaceTable	Not implemented.

IPMROUTE-STD-MIB (RFC 2932)

The IPMROUTE-STD-MIB (RFC 2932) contains objects to manage IP multicast routing, but independent of the specific multicast routing protocol in use.

MIB Constraints

Table 3-61 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the IPMROUTE-STD-MIB.

Table 3-61 IPMROUTE-STD-MIB Constraints

MIB Object	Notes
ipMRouteScopeNameTable	Not implemented.

MPLS-L3VPN-STD-MIB (RFC 4382)

The MPLS-L3VPN-STD-MIB contains managed object definitions for the Layer-3 Multiprotocol Label Switching Virtual Private Networks. This MIB is based on RFC 4382 specification.

MPLS-LDP-GENERIC-STD-MIB (RFC 3815)

The MPLS-LDP-GENERIC-STD-MIB (RFC 3815) contains managed object definitions for configuring and monitoring the Multiprotocol Label Switching Label Distribution Protocol (MPLS-LDP) and utilizing ethernet as the Layer 2 media.

MPLS-LDP-STD-MIB (RFC 3815)

The MPLS-LDP-STD-MIB (RFC 3815) contains managed object definitions for the Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP) document.

MPLS-LSR-STD-MIB (RFC 3813)

The MPLS-LSR-STD-MIB (RFC 3031) contains managed object definitions for the Multiprotocol Label Switching (MPLS) router.

MPLS-TE-STD-MIB

The MPLS-TE-STD-MIB contains managed object definitions for Multiprotocol Label Switching Traffic Engineering (MPLS-TE).

MPLS-VPN-MIB

The MPLS-VPN-MIB:

- Describes managed objects for modeling a Multiprotocol Label Switching/Border Gateway Protocol virtual private network
- Configures and monitors routes and route targets for each VRF instance on a router
- Facilitates provisioning VPN Routing and Forwarding (VRF) instances on MPLS interfaces
- Measures the performance of MPLS/BGP VPNs

The MIB is based on Revision 05 of the IETF MPLS-VPN-MIB.

MIB Constraints

Table 3-62 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the MPLS-VPN-MIB.

Table 3-62 MPLS-VPN-MIB Constraints

MIB Object	Notes
mplsNumVrfSecViolationThreshExceeded	Not implemented.
mplsVpnVrfSecTable	
• mplsVpnVrfSecIllegalLabelViolations	Read-only. Always 0.
• mplsVpnVrfSecIllegalLabelRcvThresh	Read-only. Always 0.
mplsVpnVrfTable	
• mplsVpnVrfConfRowStatus	Read-only.
• mplsVpnVrfConfStorageType	Read-only. Volatile(2).
• mplsVpnVrfConfMidRouteThreshold	Read-only.
• mplsVpnVrfConfHighRouteThreshold	Read-only
• mplsVpnVrfConfMaxRoutes	Read-only
• mplsVpnVrfConfMaxPossibleRoutes	Read-only. Always 0.
• mplsVpnVrfDescription	Read-only
• mplsVpnInterfaceVpnClassification	Read-only
mplsVpnInterfaceConfTable	
• mplsVpnInterfaceConfStorageType	Read-only. Volatile(2).
• mplsVpnInterfaceConfRowStatus	Read-only. Values: active(1), notInService(2).
• mplsVpnInterfaceLabelEdgeType	Read-only. providerEdge(1).
mplsVpnVrfRouteTargetTable	
• mplsVpnVrfRouteTargetRowStatus	Read-only. Values: active(1), notInService(2).
mplsVpnVrfBgpNbrAddrTable	
• mplsVpnVrfBgpNbrRowStatus	Read-only. Values: active(1), notInService(2).
• mplsVpnVrfBgpNbrRole	Read-only. providerEdge(1).
• mplsVpnVrfBgpNbrType	Read-only.
• mplsVpnVrfBgpNbrAddr	Read-only.

Table 3-62 MPLS-VPN-MIB Constraints (continued)

MIB Object	Notes
• mplsVpnVrfBgpNbrStorageType	Read-only. Volatile(2).
mplsVpnVrfRouteTable	
• mplsVpnVrfRouteInfo	Read-only. Value nullOID.
• mplsVpnVrfRouteTarget	Read-only. Determines the route distinguisher for this target.
• mplsVpnVrfRouteTargetDescr	Description of the route target. Currently this object is not supported in this Cisco IOS XE release. Therefore, the object is the same as mplsVpnVrfRouteTarget.
• mplsVpnVrfRouteDistinguisher	Read-only.
• mplsVpnVrfRouteNextHopAS	Read-only. Always 0.
• mplsVpnVrfRouteRowStatus	Read-only. This object normally reads active(1), but may read notInService(2), if a VRF was recently deleted.
• mplsVpnVrfRouteStorageType	Read-only. Volatile(2).
• mplsVpnVrfRouteDestAddrType	Read-only.
• mplsVpnVrfRouteMaskAddrType	Read-only.
• mplsVpnVrfRouteTos	Read-only. Always 0.
• mplsVpnVrfRouteNextHop	Read-only.
• mplsVpnVrfRouteNextHopAddrType	Read-only.
• mplsVpnVrfRouteifIndex	Read-only.
• mplsVpnVrfRouteType	Read-only.
• mplsVpnVrfRouteProto	Read-only.
mplsVpnVrfBgpNbrPrefixTable	Not implemented.

Notes:

The mplsVpnVrfConfTable represents all the MPLS/BGP VPNs configured. The NMS configures an entry in this table for each MPLS/BGP VPN configured to run in this MPLS domain. The mplsVPNInterfaceConfTable extends the interface MIB to provide specific MPLS/BGP VPN information on MPLS/BGP VPN-enabled interfaces. The mplsVPNPerfTable enhances the mplsVpnVrfConfTable to provide performance information.

The mplsVpnVrfRouteTable and the mplsVpnRouteTargetTable facilitate the configuration and monitoring of routes and route targets, respectively, for each VRF instance.

MSDP-MIB

The MSDP-MIB contains objects to monitor the Multicast Source Discovery Protocol (MSDP). The MIB can be used with SNMPv3 to remotely monitor MSDP speakers.

For more information about this MIB, see its feature module description at the following URL:

http://www.cisco.com/en/US/docs/ios/12_1t/12_1t5/feature/guide/dt5msdp.html

NHRP-MIB

The Cisco NHRP MIB feature introduces support for the NHRP MIB, which helps to manage and monitor the Next Hop Resolution Protocol (NHRP) through the Simple Network Management Protocol (SNMP). Statistics can be collected and monitored through standards-based SNMP techniques (get operations) to query objects defined in the NHRP MIB. The NHRP MIB is VRF-aware and supports VRF-aware queries.

For more information about this MIB, refer:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_dmvpn_nhrp_mib.html

MIB Constraints

Table 3-63 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the NHRP-MIB.

Table 3-63 NHRP-MIB Constraints

MIB Object	Notes
nhrpClientNbmaSubaddr	Not implemented.
nhrpClientNhsNbmaSubaddr	Not implemented.
nhrpServerNbmaSubaddr	Not implemented.
nhrpServerNhcNbmaSubaddr	Not implemented.
nhrpCachePreference	Not implemented.
nhrpClientDefaultMtu	Not implemented.
nhrpCacheNegotiatedMtu	Not implemented.
nhrpPurgePrefixLength	Not implemented.
nhrpCacheNbmaSubaddr	Not supported.
nhrpCacheType	
• atmarp(7)	Not supported.
• scsp(8)	Not supported.

NOTIFICATION-LOG-MIB (RFC 3014)

The NOTIFICATION-LOG-MIB contains objects for logging SNMP notifications; that is, traps and informs types of notifications.

OSPF-MIB (RFC 1850)

The OSPF-MIB (RFC 1850) contains objects that describe the OSPF Version 2 Protocol. The RFC1253-MIB corresponds to the OSPF-MIB (Open Shortest Path First [OSPF] protocol).

OSPF-TRAP-MIB (RFC 1850)

The OSPF-TRAP-MIB (RFC 1850) contains objects that describe traps for the OSPF Version 2 Protocol.

PIM-MIB (RFC 2934)

The PIM-MIB (RFC 2934) contains objects to configure and manage Protocol Independent Multicast (PIM) on the router. The MIB is extracted from RFC 2934.

MIB Constraints

Table 3-64 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the PIM-MIB.

Table 3-64 PIM-MIB Constraints

MIB Object	Notes
pimIpMRouteTable	Not implemented.
pimIpMRouteNextHopTable	Not implemented.
pimInterfaceTable	
• pimInterfaceMode	Read-only.
• pimInterfaceHelloInterval	Read-only.
• pimInterfaceStatus	Read-only.
• pimInterfaceJoinPruneInterval	Read-only.
• pimInterfaceCBSRPreference	Read-only.
pimJoinPruneInterval	Read-only.
pimCandidateRPTable	
• pimCandidateRPAdressd	Read-only.
• pimCandidateRPRowStatus	Read-only.
pimComponentTable	
• pimComponentCRPHoldTime	Read-only.
• pimComponentStatus	Read-only.

RFC1213-MIB

The RFC1213-MIB defines the second version of the Management Information Base (MIB-II) for use with network-management protocols in TCP-based internets. This RFC1213-MIB includes the following groups :

- system
- interfaces

- at
- ip
- icmp
- tcp
- udp
- igmp
- transmission
- snmp

Note For more information, refer to the latest RFCs specified in the RFC-1213-MIB.

RFC2982-MIB

The RFC2982-MIB defines expressions of MIB objects for management purposes.

RFC2006-MIB (MIP)

The RFC2006-MIB is the MIB module for the Mobile IP standard.

RMON-MIB (RFC 1757)

The RMON-MIB (RFC 1757) contains objects to remotely monitor devices in the network.

MIB Constraints

Only alarm and event groups are supported in Cisco ASR 903 Series Router.

RMON2-MIB (RFC 2021)

The RMON2-MIB contains objects to manage remote monitoring device implementations. This MIB module enhances the original RMON MIB as specified in RFC 2021.

RSVP-MIB

The RSVP-MIB contains objects to manage the Resource Reservation Protocol (RSVP).

SMON-MIB

The SMON-MIB contains objects to manage remote monitoring device implementations for switched networks. It identifies the source of the data that the associated function is configured to analyze. The textual convention extends the data source textual convention defined by RMON 2 to the following data source types:

- ifIndex
- smonVlanDataSource
- entPhysicalEntry

SNMP-COMMUNITY-MIB (RFC 2576)

The SNMP-COMMUNITY-MIB (RFC 2576) contains objects that help support coexistence among SNMPv1, SNMPv2c, and SNMPv3.

SNMP-FRAMEWORK-MIB (RFC 2571)

The SNMP-FRAMEWORK-MIB (RFC 2571) contains objects that describe the SNMP management architecture. There are no constraints on this MIB.

SNMP-MPD-MIB (RFC 2572)

The SNMP-MPD-MIB (RFC 2572) contains objects for Message Processing and Dispatching (MPD).

SNMP-NOTIFICATION-MIB (RFC 2573)

The SNMP-NOTIFICATION-MIB (RFC 2573) contains managed objects for SNMPv3 notifications. The MIB also defines a set of filters that limit the number of notifications generated by a particular entity (snmpNotifyFilterProfileTable and snmpNotifyFilterTable).

Objects in the snmpNotifyTable are used to select entities in the SNMP-TARGET-MIB snmpTargetAddrTable and specify the types of SNMP notifications those entities are to receive.

SNMP-PROXY-MIB (RFC 2573)

The SNMP-PROXY-MIB (RFC 2573) contains managed objects to remotely configure the parameters used by an SNMP entity for proxy forwarding operations. The MIB contains a single table, snmpProxyTable, which defines the translations to use to forward messages between management targets.

SNMP-TARGET-MIB (RFC 2573)

The SNMP-TARGET-MIB (RFC 2573) contains objects to remotely configure the parameters used by an entity to generate SNMP notifications. The MIB defines the addresses of entities to send SNMP notifications to, and contains a list of tag values that are used to filter the notifications sent to these entities (see the SNMP-NOTIFICATION-MIB).

SNMP-USM-MIB (RFC 2574)

The SNMP-USM-MIB (RFC 2574) contains objects that describe the SNMP user-based security model.

SNMPv2-MIB (RFC 1907)

The SNMPv2-MIB (RFC 1907) contains objects to manage SNMPv2 entities. The SNMPv2-MIB contains the following mandatory object groups:

- SNMP group—Collection of objects providing basic instrumentation and control of an SNMP entity.
- System group—Collection of objects common to all managed systems.
- snmpSetGroup—Collection of objects that allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation.
- snmpBasicNotificationsGroup—The two notifications are coldStart and authenticationFailure, which an SNMPv2 entity is required to implement.

SNMPv2-SMI

The SNMPv2-SMI is based on RFC1902 and describes the management information structure for Simple Network Management Protocol version 2 (SNMPv2).

SNMP-VIEW-BASED-ACM-MIB (RFC 2575)

The SNMP-VIEW-BASED-ACM-MIB (RFC 2575) contains objects that describe the view-based access control model for SNMP.

To access the SNMP-VIEW-BASED-ACM-MIB, you must create an SNMPv3 user with access to a view that includes all of the information from the Internet subtree. For example:

Router(config)# **snmp-server view abcview internet included**
Router(config)# **snmp-server group abcgroup v3 noauth read abcview write abcview notify** *abcview*
Router(config)# **snmp-server user abcuser abcgroup** *v3*

Note *Router(config)#* **snmp-server user abcuser abcgroup** *v3*

SONET-MIB (RFC 2558)

The SONET-MIB (RFC 2558) provides both the configuration and performance monitoring objects for the SONET interfaces.

MIB Constraints

Table 3-65 lists the constraints that the Cisco ASR 903 Series Router places on the objects in the SONET-MIB.

Table 3-65 SONET-MIB Constraints

MIB Object	Notes
sonetPathCurrentTable	
• sonetPathCurrentWidth	Read only.
sonetVTCurrentTable	Not implemented.
sonetVTIntervalTable	Not implemented.
sonetFarEndVTCurrentTable	Not implemented.
sonetFarEndVTIntervalTable	Not implemented.
SonetMediumTable	
• sonetMediumLineCoding	Read-Only
• sonetMediumLineType	Read-Only
• sonetMediumCircuitIdentifier	Read-Only
• sonetMediumLoopbackConfig	Read-Only
sonetSESthresholdSet	Read-Only

Note When the SONET path is initialized and no active alarms exist, the value of the sonetPathCurrentStatus object is 0. If an alarm is triggered and cleared, the value of the sonetPathNoDefect object is 1.

TCP-MIB (RFC 4022)

The TCP-MIB (RFC 4022) contains objects to manage the Transmission Control Protocol (TCP) implementations on the router.

TUNNEL-MIB (RFC 4087)

The TUNNEL-MIB contains objects to manage IP Tunnels independent of the encapsulation scheme in use.

UDP-MIB (RFC 4113)

The UDP-MIB (RFC4113) contains objects to manage the User Datagram Protocol (UDP) on the router. There are no constraints.

VRRP-MIB

The VRRP-MIB contains objects to manage Virtual Router Redundancy Protocol (VRRP) routers.

CHAPTER 4

Monitoring Notifications

This chapter describes the Cisco ASR 903 Series Aggregation Services Routers notifications supported by the MIB enhancements feature. The notifications are traps or informs for different events. The router also supports other notifications not listed.

This chapter contains the following sections:

SNMP Notification Overview

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 one of the following:

- Traps—Unreliable messages, which do not require receipt acknowledgement 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.

To use SNMP notifications on your system, you must specify their recipients. These recipients indicate where Network Registrar notifications are directed. By default, all notifications are enabled, but no recipients are defined. Until you define the recipients, no notifications are sent.

Many commands use the key 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 traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. The types of traps can be specified in command.

Note Most notification types are disabled by default. However, some notification types cannot be controlled with the **snmp** command. For example, some notification types are always enabled and other types are enabled by a different command. The linkUpDown notifications are controlled by the **snmp trap link-status** command. If you enter this command with no notification-type keywords, the default is to enable all notification types controlled by the command.

Specify the trap types if you do not want all traps to be sent. Then use multiple **snmp-server enable traps** commands, one for each of the trap types that you used in the **snmp host** command.

For detailed information about notifications and a list of notification types, go to the following URLs:

- http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.html
- http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpprox.html
- http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/xdsl.html
- http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
- http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

Enabling Notifications

You can enable MIB notifications using either of the following procedures:

- Using the command-line interface (CLI)—Specify the recipient of the trap message and specify the types of traps sent and the types of informs that are enabled. For detailed procedures, go to:
  - http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
  - http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.html
- Performing an SNMP SET operation with the **setany** command—To enable or disable MIB notifications, perform an SNMP SET operation on a specific object.
  - To enable the notifications set the object to true(1)
  - To disable the notifications, set the object to false(2)

Note If you issue the **snmp-server enable traps** command without a notification-type argument, the router generates traps for all types of events, which might not be desirable. Some MIBs require the user to set additional objects to enable some notifications.

Cisco SNMP Notifications

This section contains tables that describe a MIB event, why the event occurred, and a recommendation as to how to handle the event. Each table lists the following information:

- Events—The event display
- Description—What the event indicates
- Probable cause—What might have caused the notification
- Recommended action—Recommendation as to what should be done when the particular notification occurs

Note In the following tables, where "No action is required." appears in the Rcommended Action column, there might be instances where an application, such as trouble ticketing occurs. Environmental or Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco ASR 903 Series Router or conditions that might affect router functionality.

Table 4-1 Environmental or Functional Notifications

Event	Description	Probable Cause	Recommended Action
cefcModuleStatusChange	Indicates that the status of a module has changed.	Module has unknown state.	Enter the **show platform** command to view error message details. For syslog messages associated with this event, consult Messages and Recovery procedures.
		Module is operational.	No action is required.
		Module has failed due to some condition.	Enter the **show platform** command to view error message details. For Syslog messages associated with this event, consult Messages and Recovery Procedures.
cefcPowerStatusChange	Indicates that the power status of a field-replaceable unit (FRU) has changed.	The FRU is powered off because of an unknown problem.	Enter the **show power** command to check the actual power usage. For syslog messages associated with this event, consult Messages and Recovery Procedures
		FRU is powered on.	No action is required.
		FRU is administratively off.	No action is required.
		FRU is powered off because available system power is insufficient.	Enter the **show power** command to check the actual power usage.
cefcFRUInserted	Indicates that a FRU was inserted.	A new FRU, such as Cisco ASR 903 Series Router Switch Processor 1 (RSP 1), interface module, fan, transceiver, power supply, or redundant power supply was added.	No action is required.
cefcFRURemoved	Indicates that a FRU was removed.	A FRU, such as RSP1, interface module, fan, transceiver, power supply, or redundant power supply was removed.	Replace the FRU.

Table 4-1 Environmental or Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
dsx1LineStatusChange	The dsx1LineStatus is a bit-map that contains loopback state and failure state information.	When a failure is detected, the corresponding dsx1LineStatus bit should change to reflect the failure. For example, when a Receiving LOS failure is detected, the corresponding bit (bit 64) should be set to indicate the failure and as a result, the dsx1LineStatus should change.	When the dsx1LineStatus reports a failure, the recommended action is correction of the conditions causing the error.
cdcVFileCollectionError	Indicates that data collection operations for a cdcVFileEntry has encountered an error.		
cdcFileXferComplete	A file transfer to the destination specified by the cdcVFileMgmtLastXferURL variable, has completed with the status specified by the cdcVFileMgmtLastXferStatus variable.	File transfer complete.	No action is required.

Table 4-2 lists ENTITY-MIB notifications generated by Cisco ASR 903 Series Router RSP cards.

Table 4-2 RSP Card Notifications

Event	Description	Probable Cause	Recommended Action
entConfigChange	An entry for the transceiver module is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change).	A transceiver module was removed.	Replace the FRU.
entSensorThresholdNotification	Indicates that the sensor value crossed the threshold. This variable reports the most recent measurement seen by the sensor and the threshold value.	The sensor value in a module crossed the threshold listed in entSensorThresholdTable. This notification is generated once each time the sensor value crosses the threshold.	Remove the configuration that bypasses the module shutdown due to sensor thresholds being exceeded. Shut down the module after removing the configuration. It exceeded major sensor thresholds. **Note** The command that shuts down the module in the event of a major sensor alarm has been overridden, so the specified module will not be shut down. The command used to override the shutdown is **no environment-monitor shutdown**.
		The local CPU on the RSP was unable to access the temperature sensor on the module. The module will attempt to recover by resetting itself.	Copy the error message exactly as it appears on the console or in the system log, contact your Cisco technical support representative, and provide the representative with the gathered information.
ceAlarmAsserted	The agent generates this trap when a physical entity asserts an alarm.	You manually shut down the IM, then you get the IM error.	Check the entPhysicalDescr type and take the corresponding action; there are many types of asserted alarms.

Table 4-2 RSP Card Notifications (continued)

Event	Description	Probable Cause	Recommended Action
ceAlarmCleared	The agent generates this trap when a physical entity clears a previously asserted alarm.	The agent generates this trap when a physical entity clears a previously asserted alarm.	No action is required.

Notes:

Sensor entities are the physical entities whose entity class must be defined to type entity sensor(8) in the entPhysicalTable.

Notifications happen only if the particular entity has an entry in the entity table.

If ceAlarmNotifiesEnable is set to 0, it disables ceAlarmAsserted and ceAlarmCleared notifications. Similarly, when ceAlarmSyslogEnable is set to 0, it disables syslog messages corresponding to alarms.

If ceAlarmHistTableSize is set to 0, it prevents any history from being retained in the ceAlarmHistTable. In addition, whenever the ceAlarmHistTableSize is reset (either increased or decreased), the existing log is deleted..

Flash Device Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco ASR 903 Series Router flash devices. These notifications indicate the failure of a flash device or error conditions on the device.

Table 4-3 Flash Device Notifications

Event	Description	Probable Cause	Recommended Action
ciscoFlashDeviceChangeTrap	Indicates a removable flash device was inserted into the router.	Status change occurred.	To determine which flash device was inserted, check the ciscoFlashDeviceTable.
	Indicates removable flash device was removed from the router.	Status change occurred.	To determine which flash device was removed, check the ciscoFlashDeviceTable.

Interface Notifications

Table 4-4 lists notifications generated by the router for link-related (interface) events.

Table 4-4 Interface Notifications

Event	Description	Probable Cause	Recommended Action
linkDown	Indicates that a link is about to enter the down state, which means it cannot transmit or receive traffic. The ifOperStatus object shows the previous state. Value is down(2).	An internal software error might have occurred.	To see if link traps are enabled or disabled on an interface, check ifLinkUpDownTrapEnable (IF-MIB) for the interface. To enable link traps, set ifLinkUpDownTrapEnable to enabled(1). Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**.
linkUp	Indicates that a link is no longer down. The value of ifOperStatus indicates the link's new state. Value is up(1).	The port manager reactivated a port in the down state during a switchover.	No action is required.

Cisco MPLS Notifications

Table 4-5 lists MPLS-VPN notifications that can occur when an environmental threshold is exceeded.

Table 4-5 MPLS-VPN Notifications

Event	Description	Probable Cause	Recommended Action
mplsNumVrfRouteMidThreshExceeded	Indicates that the warning threshold is exceeded. Indicates that a threshold violation occurred.	The system limit of four Route Switch Processors per VPN has been exceeded. The number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.	The configured RSPs are too large to fit in the DF table for one VPN. Try to configure the groups among existing RSPs in the hardware, or configure the RSP in another VPN.

Table 4-5 MPLS-VPN Notifications (continued)

Event	Description	Probable Cause	Recommended Action
mplsNumVrfRouteMaxThreshExceeded	Indicates that the maximum route limit was reached.	A route creation was unsuccessful because the maximum route limit was reached. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.	Set the threshold value. The maximum-threshold value is determined by the **maximum routes** command in VRF configuration mode.
mplsLdpFailedInitSessionThreshold Exceeded	Indicates that a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts.	Eight failed attempts occurred to establish an LDP session between a local LSR and an LDP peer due to some type of incompatibility between the devices. Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.	If you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated and sent to the NMS as an informational message. Operationally, the LSRs with label ranges that do not overlap continue their attempts to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

Service Notifications

Table 4-6 lists MPLS-Service notifications generated by the router to indicate conditions for services.

Table 4-6 MPLS Service Notifications

Event	Description	Probable Cause	Recommended Action
mplsVrfIfUp	Indicates that a VPN routing or forwarding instance (VRF) was assigned to an interface that is operational or for the transition of a VRF interface to the operationally up state.	A VPN routing or forwarding instance (VRF) was assigned to an interface that is operational or a VRF interface transitions to the up state.	No action is required.
mplsVrfIfDown,	Indicates that a VRF was removed from an interface or a VRF interface transitioned to the operationally down state.	A VRF was removed from an interface or a VRF of an interface transitioned to the down state.	Check the operation state of the interface Or the state of the connected interface on the adjacent router Or add the removed VRF.
mplsLdpSessionUp	Indicates that the MPLS LDP session is in the up state.	Trap generated when an LDP entity (a local LSR) establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).	No action is required.
mplsLdpSessionDown	Indicates that the MPLS LDP session is in the down state.	Trap generated when an LDP session between a local LSR and its adjacent LDP peer is terminated.	Check if the LDP session exists between the local LSR and adjacent LDP peer.
mplsLdpPVLMismatch	Indicates that a local LSR establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.	An LDP session has two adjacent peer LSRs with dissimilar path vector limits. The value of the path vector limit can range from 0 through 255; a value of “0” indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on.	Configure all LDP-enabled routers in the network with the same path vector limit. Accordingly, the mplsLdpPathVectorLimitMismatch object exists in the MPLS-LDP-MIB to provide a warning message to the NMS when two routers engaged in LDP operations have a dissimilar path vector limit.
mplsTunnelUp	Indicates that a mplsTunnelOperStatus object for a configured tunnel is about to transition from the down state to any state except NotPresent.	A configured tunnel transitioned from the down state to any state except NotPresent. May be caused by an administrative or operational status check of the tunnel.	No action is required.

Table 4-6 MPLS Service Notifications (continued)

Event	Description	Probable Cause	Recommended Action
mplsTunnelDown	Indicates that the mplsTunnelOperStatus object for a configured MPLS traffic engineering tunnel is about to transition to the up(1) or the down(2) state respectively.	A configured tunnel is transitioning to the down state. May be caused by an administrative or operational status check of the tunnel.	
mplsTunnelRerouted	Indicates that the signalling path for an MPLS traffic engineering tunnel changed.	A tunnel was rerouted or reoptimized.	If you use the actual path, then write the new path to mplsTunnelRerouted after the notification is issued.

Routing Protocol Notifications

Table 4-7 lists BGP4-MIB notifications that are Border Gateway Protocol (BGP) state changes generated by the Cisco ASR 903 Series Router to indicate error conditions for routing protocols and services.

Table 4-7 Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
bgpEstablished	The BGP FSM enters the Established state. It becomes active on the router.	BGP changed status.	No action is required.
bgpBackwardTransition	Indicates that BGP transitions from a higher-level state to a lower-level state. The prefix count for an address family on a BGP session exceeded the configured threshold value.	BGP changed status.	This threshold value is configured using the CLI command **neighbor** *nbr_addr max_prefixes* [threshold] [warning-only].

RTT Monitor Notifications

Table 4-8 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

Table 4-8 RTT Monitor Notifications

Event	Description	Probable Cause	Recommended Action
rttMonConnectionChangeNotification	Sent when the value of rttMonCtrlOperConnectionLostOccurred changes.	Occurs when the connection to a target has either failed to be established or was lost and then re-established.	Check for the connectivity to the target. There could be link problems to the target through different hops.
rttMonTimeoutNotification	A timeout occurred or was cleared.	An RTT probe occurred and the system sends the notice when the value of rttMonCtrlOperTimeoutOccurred changes.	Check for the end-to-end connectivity if rttMonCtrlOperTimeoutOccurred in the notification returns true. No action is required if rttMonCtrlOperTimeoutOccurred is false.
rttMonThresholdNotification	Threshold violation occurred.	An RTT probe occurred or a previous violation has subsided in a subsequent RTT operation.	Check for the end-to-end connectivity if rttMonCtrlOperOverThresholdOccurred in the notification is true; otherwise, no action is required.

Redundancy Framework Notifications

Table 4-9 lists CISCO-RF-MIB notifications that can occur in a redundant system. There are two types of notifications:

- Switch of Activity (SWACT)—Either a forced or automatic switch of active status from the active unit to the standby unit. The former standby unit is now referred to as the active unit.
- Progression—The process of making the redundancy state of the standby unit equivalent to that of the active unit. This includes transitioning the RF state machine through several states, which drives the RF clients on the active unit to synchronize any relevant data with their peer on the standby unit.

Table 4-9 Redundancy Framework Notifications

Event	Description	Probable Cause	Recommended Action
ciscoRFSwactNotif	Indicates that the RF state changed. A switch of activity notification is sent by the newly active redundant unit.	A switch of activity occurs. If a SWACT event is indistinguishable from a reset event, then a network management station should use this notification to differentiate the activity.	If the switchover occurred because the active unit failed (indicated by cRFStatusLastSwactReasonCode) see if there are any hardware failures; otherwise, no action is required.
ciscoRFProgressionNotif	Indicates that the RF state changed.	The active redundant unit RF state changed or the RF state of the peer unit changed.	To avoid an increase of notifications for all state transitions, send notifications for transitions to the following RF states: • standbyCold(5) • standbyHot(9) • active(14) • activeExtraload(15)

CPU Usage Notifications

The Cisco ASR 903 Series Router does not support CPU Usage Notifications. To generate notification for the cpu threshold, you can use RMON-MIB alarm and event in conjunction with CISCO-PROCESS-MIB object which represents the CPU.

APPENDIX A

Using MIBs

This chapter describes how to perform tasks on the Cisco ASR 903 Series Aggregation Services Routers:

Cisco Unique Device Identifier Support

The ENTITY-MIB now supports the Cisco compliance effort for a Cisco unique device identifier (UDI) standard which is stored in IDPROM.

The Cisco UDI provides a unique identity for every Cisco product. The UDI is composed of three separate data elements which must be stored in the entPhysicalTable:

- Orderable product identifier (PID)—Product Identifier (PID). PID is the alphanumeric identifier used by customers to order Cisco products. Two examples include NM-1FE-TX or CISCO3745. PID is limited to 18 characters and must be stored in the entPhysicalModelName object.
- Version identifier (VID)—Version Identifier (VID). VID is the version of the PID. The VID indicates the number of times a product has versioned in ways that are reported to a customer. For example, the product identifier NM-1FE-TX may have a VID of V04. VID is limited to three alphanumeric characters and must be stored in the entPhysicalHardwareRev object.
- Serial number (SN)—Serial number is the 11-character identifier used to identify a specific part within a product and must be stored in the entPhysicalSerialNum object. Serial number content is defined by manufacturing part number 7018060-0000. The SN is accessed at the following website by searching on the part number 701806-0000:

  https://mco.cisco.com/servlet/mco.ecm.inbiz

  Serial number format is defined in four fields:

  - Location (L)
  - Year (Y)
  - Workweek (W)

- Sequential serial ID (S)

The SN label is represented as: LLLYYWWSSS.

Note The Version ID returns NULL for those old or existing cards whose IDPROMs do not have the Version ID field. Therefore, corresponding entPhysicalHardwareRev returns NULL for cards that do not have the Version ID field in IDPROM.

Cisco Redundancy Features

Redundancy creates a duplication of data elements and software functions to provide an alternative in case of failure. The goal of Cisco redundancy features is to cut over without affecting the link and protocol states associated with each interface and continue packet forwarding. The state of the interfaces and subinterfaces is maintained, along with the state of line cards and various packet processing hardware.

The levels of redundancy, redundancy verification, and related informatin is covered in these sections:

Levels of Redundancy

Cisco ASR 903 Series Router supports fault resistance by allowing a Cisco redundant Supervisor Engine (SE) to take over if the active SE fails. Redundancy prevents equipment failures from causing service outages, and supports hitless maintenance and upgrade activities. The state of the interfaces and subinterfaces are maintained along with the state of line cards and various packet processing hardware.

Redundant systems support two route switch processors. One acts as the active route switch processor while the other acts as the standby.

The route switch processor redundancy feature provides high availability for Cisco routers by switching over to the standby route switch processor when one of the following conditions occur:

- Cisco IOS XE software failure
- Cisco ASR 903 Series Route Switch Processor (RSP) hardware failure
- Software upgrade
- Maintenance procedure

Cisco ASR 903 Series Router can operate in one of two redundancy modes:

- Route Switch Processor Redundancy (RPR) Mode
- Cisco Nonstop Forwarding and Stateful Switchover (NSF/SSO)

In all modes, the standby RSP will take over when the active RSP fails.

Route Switch Processor Redundancy (RPR) Mode

This section describes the Route Processor Redundancy (RPR) mode for the Cisco ASR 903 Series Router.

When the switch is powered on, RPR runs between two Cisco SEs. The supervisor engine that boots first becomes the RPR active SE.

Cisco ASR 903 Series Router supports fault resistance by allowing a redundant SE to take over if the active SE fails.

Cisco Nonstop Forwarding and Stateful Switchover (NSF/SSO)

This section describes the Cisco Nonstop Forwarding and Stateful switchover mode. With Cisco NSF/SSO, Cisco ASR 903 Series Router can fail over from the active to the standby route switch processor almost immediately while continuing to forward packets. Cisco IOS XE software with Cisco NSF/SSO support on this platform enables immediate failover.

In networking devices running Cisco NSF/SSO, both RSPs must be running the same configuration so that the standby RSP is always ready to assume control following a fault on the active RSP. The configuration information is synchronized from the active RSP to the standby RSP at startup and each time when changes to the active RSP configuration occur.

Following an initial synchronization between the two processors, NFS/SSO maintains RSP state information between them, including forwarding information.

Cisco NSF works with the SSO to minimize the amount of time a network is unavailable to its users following a RSP failover in a router with dual RSPs. The Cisco NSF/SSO capability allows routers to detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from peer devices.

Note For detailed information about the Cisco Nonstop Forwarding feature, go to: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnsf20s.html

Note For detailed information about the Stateful Switchover feature, go to: http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html

Verifying Cisco ASR 903 Series Router Redundancy

To display information about the active and standby SE installed on a Cisco ASR 903 Series Router, use the **show redundancy** and **show redundancy states** commands. For RSP in R0 slot, the value of Unit ID is 48, same as ASCII "0" (hex 30). The value of Unit ID is 49, ASCII "1" (hex 31), for RSP in R1 slot.

Example A-1 Displaying Redundancy States from Active Processor

```
Router#show redundancy states
```

```
my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
           Unit = Primary
        Unit ID = 48

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
    Manual Swact = enabled
 Communications = Up

   client count = 87
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0


Router#exit
```

Example A-2 Displaying Redundancy States from Standby Processor

```
Router#show redundancy state
my state = 8  -STANDBY HOT
     peer state = 13 -ACTIVE
           Mode = Duplex
           Unit = Secondary
        Unit ID = 49

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
    Manual Swact = cannot be initiated from this the standby unit
 Communications = Up

   client count = 87
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

Router#
```

Related Information and Useful Links

The following URLs provide access to helpful information about the Cisco redundancy feature:

- Detailed information about Cisco Nonstop Forwarding:
  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fsnsf20s.html
- Detailed information about the Stateful Switchover Feature:
  http://www.cisco.com/en/US/docs/ios/12_2s/feature/guide/fssso20s.html
- Detailed information about the Route Processor Redundancy Feature:
  http://www.cisco.com/en/US/docs/ios/12_1/12_1ex/feature/guide/12e_rpr.html

Managing Physical Entities

This section describes how to use SNMP to manage the physical entities (components) in the router by:

- Performing Inventory Management, page A-6

Purpose and Benefits

The physical entity management feature of the Cisco ASR 903 Series Router SNMP implementation does the following:

- Monitors and configures the status of field replaceable units (FRUs)
- Provides information about physical port to interface mappings
- Provides asset information for asset tagging
- Provides firmware and software information for chassis components

MIBs Used for Physical Entity Management

- CISCO-ENTITY-FRU-CONTROL-MIB—Contains objects used to monitor and configure the administrative and operational status of field replaceable units (FRUs), such as power supplies and line cards, that are listed in the entPhysicalTable of the ENTITY-MIB.
- CISCO-ENTITY-EXT-MIB - Contains Cisco defined extensions to the entPhysicalTable of the ENTITY-MIB to provide information for entities with an entPhysicalClass value of 'module' that have a CPU, RAM/NVRAM, and/or a configuration register.
- CISCO-ENTITY-SENSOR-MIB and ENTITY-SENSOR-MIB—Contain information about entities in the entPhysicalTable with an entPhysicalClass value of 'sensor'.
- CISCO-ENTITY-VENDORTYPE-OID-MIB—Contains the object identifiers (OIDs) for all physical entities in the router.
- ENTITY-MIB—Contains information for managing physical entities on the router. It also organizes the entities into a containment tree that depicts their hierarchy and relationship to each other. The MIB contains the following tables:
  - The entPhysicalTable describes each physical component (entity) in the router. The table contains an entry for the top-level entity (the chassis) and for each entity in the chassis. Each entry provides information about that entity: its name, type, vendor, and a description, and describes how the entity fits into the hierarchy of chassis entities.

    Each entity is identified by a unique index (*entPhysicalIndex*) that is used to access information about the entity in this and other MIBs.
  - The entAliasMappingTable maps each physical port's entPhysicalIndex value to its corresponding ifIndex value in the IF-MIB ifTable.
  - The entPhysicalContainsTable shows the relationship between physical entities in the chassis. For each physical entity, the table lists the entPhysicalIndex for each of the entity's child objects.
  - The entPhysicalIsFRU indicates whether or not a physical entity is considered a Field Replaceable Unit (FRU). For an entity identified as FRU, the physical entity contains the following device-specific information:
    - entPhysicalModelName- Product Identification (PID), same as orderable part number.
    - entPhysicalHardwareRev- Version Identification (VID)
    - entPhysicalSerialNum- Serial Number (SN)

- Cisco Unique Device Identifier (UDI)- Composed of PID, VID and SN, it provides a unique identity for all Cisco hardware products on which it has been enabled.

Performing Inventory Management

To obtain information about entities in the router, perform a MIB walk on the ENTITY-MIB entPhysicalTable.

As you examine sample entries in the ENTITY-MIB entPhysicalTable, consider the following:

- entPhysicalIndex—Uniquely identifies each entity in the chassis. This index is also used to access information about the entity in other MIBs.
- entPhysicalContainedIn—Indicates the entPhysicalIndex of a component's parent entity.
- entPhysicalParentRelPos—Shows the relative position of same-type entities that have the same entPhysicalContainedIn value (for example, chassis slots, and line card ports).

Note The container is applicable if the physical entity class is capable of containing one or more removable physical entities. For example, each (empty or full) slot in a chassis is modeled as a container. All removable physical entities should be modeled within a container entity, such as field-replaceable modules, fans, or power supplies.

ENTITY-MIB

The Entity physical table contains information for managing physical entities on the router. It also organizes the entities into a containment tree that depicts their hierarchy, and relationship with each other. Refer to the Appendix A, "Entity Containment Tree" section for the entity hierarchy. The following sample output contains the information for the ASR 903 AC power supply in power supply bay 0:

```
sw-mrrbu-nms-1:/opt/ats/ats5.1.0>getmany -v2c 10.86.0.50 public entityMIB | grep "\.11 ="
| more
entPhysicalDescr.11 = ASR 900 500W DC Power Supply
entPhysicalVendorType.11 = cevPowerSupply.332
entPhysicalContainedIn.11 = 10
entPhysicalClass.11 = powerSupply(6)
entPhysicalParentRelPos.11 = 0
entPhysicalName.11 = Power Supply Module 0
entPhysicalHardwareRev.11 = V00
entPhysicalFirmwareRev.11 =
entPhysicalSoftwareRev.11 =
entPhysicalSerialNum.11 =
entPhysicalMfgName.11 = Cisco Systems Inc
entPhysicalModelName.11 = A900-PWR550-D
entPhysicalAlias.11 =
entPhysicalAssetID.11 =
entPhysicalIsFRU.11 = true(1)
entPhysicalMfgDate.11 = 00 00  00 00   00 00  00 00
entPhysicalUris.11 = URN:CLEI:UNASSIGNED
entPhysicalChildIndex.10.11 = 11
sw-mrrbu-nms-1:/opt/ats/ats5.1.0>
```

For more information on this MIB, refer to ENTITY-MIB (RFC 4133), page 3-54.

Entity Containment Tree

The following is sample entity hierarchy for a ASR 903 device, with Mib Variables printed : <entPhysicalName entPhysicalClass>

```
ENTITY-MIB containment tree:
    |
|
    \-1 (cevChassis.1120) : Chassis : ASR 903 Series Router Chassis : ASR-903 : chassis
         |
         +-2 (cevContainer.246) : slot R0 : RSP Slot : {} : container
         |    |
         |    \-100 (cevModule.87.1) : module R0 : ASR 900 Route Switch Processor 1,
55Gbps throughput : A900-RSP1A-55 : module
         |         |
         |         +-101 (cevSensorModuleDeviceVoltage) : VNILE: VX1 R0/0 : VNILE: VX1 :
{} : sensor
         |         |
         |         +-102 (cevSensorModuleDeviceVoltage) : VNILE: VX2 R0/1 : VNILE: VX2 :
{} : sensor
         |         |
         |         +-103 (cevSensorModuleDeviceVoltage) : VNILE: VX3 R0/2 : VNILE: VX3 :
{} : sensor
         |         |
         |         +-104 (cevSensorModuleDeviceVoltage) : VNILE: VX4 R0/3 : VNILE: VX4 :
{} : sensor
         |         |
         |         +-105 (cevSensorModuleDeviceVoltage) : VNILE: VP1 R0/4 : VNILE: VP1 :
{} : sensor
         |         |
         |         +-106 (cevSensorModuleDeviceVoltage) : VNILE: VP2 R0/5 : VNILE: VP2 :
{} : sensor
         |         |
         |         +-107 (cevSensorModuleDeviceVoltage) : VNILE: VP3 R0/6 : VNILE: VP3 :
{} : sensor
         |         |
         |         +-108 (cevSensorModuleDeviceVoltage) : VNILE: VH R0/7 : VNILE: VH : {}
: sensor
         |         |
         |        +-109 (cevSensorModuleDeviceTemp) : Temp: Nile 0   R0/8 : Temp: Nile 0
: {} : sensor
         |         |
         |        +-110 (cevSensorModuleDeviceTemp) : Temp: N-Inlet  R0/9 : Temp: N-Inlet
: {} : sensor
         |         |
         |        +-111 (cevSensorModuleDeviceTemp) : Temp: Nile 1   R0/10 : Temp: Nile 1
: {} : sensor
         |         |
         |         +-112 (cevSensorModuleDeviceTemp) : Temp: N-Outlet R0/11 : Temp:
N-Outlet : {} : sensor
         |         |
         |         +-113 (cevSensorModuleDeviceVoltage) : VCPU : VX1 R0/12 : VCPU : VX1 :
{} : sensor
         |         |
         |         +-114 (cevSensorModuleDeviceVoltage) : VCPU : VX2 R0/13 : VCPU : VX2 :
{} : sensor
         |         |
         |         +-115 (cevSensorModuleDeviceVoltage) : VCPU : VX3 R0/14 : VCPU : VX3 :
{} : sensor
         |         |
         |         +-116 (cevSensorModuleDeviceVoltage) : VCPU : VX4 R0/15 : VCPU : VX4 :
{} : sensor
         |         |
```

```
          |         +-117 (cevSensorModuleDeviceVoltage) : VCPU : VP1 R0/16 : VCPU : VP1 :
{} : sensor
          |         |
          |         +-118 (cevSensorModuleDeviceVoltage) : VCPU : VP2 R0/17 : VCPU : VP2 :
{} : sensor
          |         |
          |         +-119 (cevSensorModuleDeviceVoltage) : VCPU : VP3 R0/18 : VCPU : VP3 :
{} : sensor
          |         |
          |         +-120 (cevSensorModuleDeviceVoltage) : VCPU : VP4 R0/19 : VCPU : VP4 :
{} : sensor
          |         |
          |         +-121 (cevSensorModuleDeviceVoltage) : VCPU : VH R0/20 : VCPU : VH : {}
: sensor
          |         |
          |        +-122 (cevSensorModuleDeviceTemp) : Temp: CPU      R0/21 : Temp: CPU
: {} : sensor
          |         |
          |         +-123 (cevSensorModuleDeviceTemp) : Temp: C-Inlet  R0/22 : Temp:
C-Inlet  : {} : sensor
          |         |
          |         +-124 (cevSensorModuleDeviceTemp) : Temp: PCIe Sw  R0/23 : Temp: PCIe
Sw  : {} : sensor
          |         |
          |         +-125 (cevSensorModuleDeviceTemp) : Temp: C-Outlet R0/24 : Temp:
C-Outlet : {} : sensor
          |         |
          |         +-131 (cevModuleCpuType) : cpu R0/0 : CPU 0 of module R0 : {} : cpu
          |         |
          |         +-132 (cevPortUSB) : usb R0/0 : USB Port : {} : port
          |         |    |
          |         |    \-133 (cevUsbFlash) : usb0 : USB Flash : {} : module
          |         |
          |         +-134 (cevPortUSB) : usb R0/1 : USB Port : {} : port
          |         |
          |         \-136 (cevPortGe) : NME R0 : Network Management Ethernet : {} : port
          |
         +-3 (cevContainer.246) : slot R1 : RSP Slot : {} : container
          |
         +-4 (cevContainer.249) : subslot 0/0 : IM Bay : {} : container
          |
         +-5 (cevContainer.249) : subslot 0/1 : IM Bay : {} : container
          |    |
          |    \-550 (cevModuleCommonCards.334) : IM subslot 0/1 : 8-port Gigabit Ethernet
Interface Module : A900-IM8T : module
          |         |
          |         +-551 (cevPortGe) : GigabitEthernet0/1/0 : A900-IM8T : {} : port
          |         |
          |         +-552 (cevPortGe) : GigabitEthernet0/1/1 : A900-IM8T : {} : port
          |         |
          |         +-553 (cevPortGe) : GigabitEthernet0/1/2 : A900-IM8T : {} : port
          |         |
          |         +-554 (cevPortGe) : GigabitEthernet0/1/3 : A900-IM8T : {} : port
          |         |
          |         +-555 (cevPortGe) : GigabitEthernet0/1/4 : A900-IM8T : {} : port
          |         |
          |         +-556 (cevPortGe) : GigabitEthernet0/1/5 : A900-IM8T : {} : port
          |         |
          |         +-557 (cevPortGe) : GigabitEthernet0/1/6 : A900-IM8T : {} : port
          |         |
          |         +-558 (cevPortGe) : GigabitEthernet0/1/7 : A900-IM8T : {} : port
          |         |
          |         +-567 (cevSensorModuleDeviceTemp) : subslot 0/1 temperature Sensor 0 :
subslot 0/1 temperature Sensor 0 : {} : s+
```

```
          |         |
          |         +-568 (cevSensorModuleDeviceTemp) : subslot 0/1 temperature Sensor 1 :
subslot 0/1 temperature Sensor 1 : {} : s+
          |         |
          |         +-569 (cevSensorModuleDeviceTemp) : subslot 0/1 temperature Sensor 2 :
subslot 0/1 temperature Sensor 2 : {} : s+
          |         |
          |         +-570 (cevSensorModuleDeviceTemp) : subslot 0/1 temperature Sensor 3 :
subslot 0/1 temperature Sensor 3 : {} : s+
          |         |
          |         +-571 (cevSensorModuleDeviceTemp) : subslot 0/1 temperature Sensor 4 :
subslot 0/1 temperature Sensor 4 : {} : s+
          |         |
          |         +-579 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 0 :
subslot 0/1 voltage Sensor 0 : {} : sensor
          |         |
          |         +-580 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 1 :
subslot 0/1 voltage Sensor 1 : {} : sensor
          |         |
          |         +-581 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 2 :
subslot 0/1 voltage Sensor 2 : {} : sensor
          |         |
          |         +-582 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 3 :
subslot 0/1 voltage Sensor 3 : {} : sensor
          |         |
          |         +-583 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 4 :
subslot 0/1 voltage Sensor 4 : {} : sensor
          |         |
          |         \-584 (cevSensorModuleDeviceVoltage) : subslot 0/1 voltage Sensor 5 :
subslot 0/1 voltage Sensor 5 : {} : sensor
          |
          +-6 (cevContainer.249) : subslot 0/2 : IM Bay : {} : container
          |    |
          |    \-800 (cevModuleCommonCards.336) : IM subslot 0/2 : 16 port T1/E1 IM :
A900-IMA16D : module
          |         |
          |         +-817 (cevSensorModuleDeviceTemp) : subslot 0/2 temperature Sensor 0 :
subslot 0/2 temperature Sensor 0 : {} : s+
          |         |
          |         +-818 (cevSensorModuleDeviceTemp) : subslot 0/2 temperature Sensor 1 :
subslot 0/2 temperature Sensor 1 : {} : s+
          |         |
          |         +-819 (cevSensorModuleDeviceTemp) : subslot 0/2 temperature Sensor 2 :
subslot 0/2 temperature Sensor 2 : {} : s+
          |         |
          |         +-829 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 0 :
subslot 0/2 voltage Sensor 0 : {} : sensor
          |         |
          |         +-830 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 1 :
subslot 0/2 voltage Sensor 1 : {} : sensor
          |         |
          |         +-831 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 2 :
subslot 0/2 voltage Sensor 2 : {} : sensor
          |         |
          |         +-832 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 3 :
subslot 0/2 voltage Sensor 3 : {} : sensor
          |         |
          |         +-833 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 4 :
subslot 0/2 voltage Sensor 4 : {} : sensor
          |         |
          |         \-834 (cevSensorModuleDeviceVoltage) : subslot 0/2 voltage Sensor 5 :
subslot 0/2 voltage Sensor 5 : {} : sensor
          |
          +-7 (cevContainer.249) : subslot 0/3 : IM Bay : {} : container
```

```
         |    |
         |    \-1050 (cevModuleCommonCards.334) : IM subslot 0/3 : 8-port Gigabit Ethernet
Interface Module : A900-IM8T : module
         |         |
         |         +-1051 (cevPortGe) : GigabitEthernet0/3/0 : A900-IM8T : {} : port
         |         |
         |         +-1052 (cevPortGe) : GigabitEthernet0/3/1 : A900-IM8T : {} : port
         |         |
         |         +-1053 (cevPortGe) : GigabitEthernet0/3/2 : A900-IM8T : {} : port
         |         |
         |         +-1054 (cevPortGe) : GigabitEthernet0/3/3 : A900-IM8T : {} : port
         |         |
         |         +-1055 (cevPortGe) : GigabitEthernet0/3/4 : A900-IM8T : {} : port
         |         |
         |         +-1056 (cevPortGe) : GigabitEthernet0/3/5 : A900-IM8T : {} : port
         |         |
         |         +-1057 (cevPortGe) : GigabitEthernet0/3/6 : A900-IM8T : {} : port
         |         |
         |         +-1058 (cevPortGe) : GigabitEthernet0/3/7 : A900-IM8T : {} : port
         |         |
         |        +-1067 (cevSensorModuleDeviceTemp) : subslot 0/3 temperature Sensor 0 :
subslot 0/3 temperature Sensor 0 : {} : +
         |         |
         |        +-1068 (cevSensorModuleDeviceTemp) : subslot 0/3 temperature Sensor 1 :
subslot 0/3 temperature Sensor 1 : {} : +
         |         |
         |        +-1069 (cevSensorModuleDeviceTemp) : subslot 0/3 temperature Sensor 2 :
subslot 0/3 temperature Sensor 2 : {} : +
         |         |
         |        +-1070 (cevSensorModuleDeviceTemp) : subslot 0/3 temperature Sensor 3 :
subslot 0/3 temperature Sensor 3 : {} : +
         |         |
         |        +-1071 (cevSensorModuleDeviceTemp) : subslot 0/3 temperature Sensor 4 :
subslot 0/3 temperature Sensor 4 : {} : +
         |         |
         |         +-1079 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 0 :
subslot 0/3 voltage Sensor 0 : {} : sensor
         |         |
         |         +-1080 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 1 :
subslot 0/3 voltage Sensor 1 : {} : sensor
         |         |
         |         +-1081 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 2 :
subslot 0/3 voltage Sensor 2 : {} : sensor
         |         |
         |         +-1082 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 3 :
subslot 0/3 voltage Sensor 3 : {} : sensor
         |         |
         |         +-1083 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 4 :
subslot 0/3 voltage Sensor 4 : {} : sensor
         |         |
         |         \-1084 (cevSensorModuleDeviceVoltage) : subslot 0/3 voltage Sensor 5 :
subslot 0/3 voltage Sensor 5 : {} : sensor
         |
         +-8 (cevContainer.249) : subslot 0/4 : IM Bay : {} : container
         |
         +-9 (cevContainer.249) : subslot 0/5 : IM Bay : {} : container
         |
         +-10 (cevContainer.247) : Power Supply Bay 0 : Power Supply Bay : {} : container
         |
         +-30 (cevContainer.247) : Power Supply Bay 1 : Power Supply Bay : {} : container
         |
         \-50 (cevContainer.248) : Fan Tray Bay 0 : Fan Tray Bay : {} : container
              |
              \-51 (cevFan.178) : Fan Tray : ASR 903 FAN Tray : A903-FAN : fan
                   |
```

```
                    +-52 (cevSensorModuleDeviceTemp) : Temp: FC PWM1 P2/0 : Temp: FC PWM1 :
{} : sensor
                     |
                     +-62 (cevFan.179) : Fan 2/0 : Fan : {} : fan
                     |
                     +-63 (cevFan.179) : Fan 2/1 : Fan : {} : fan
                     |
                     +-64 (cevFan.179) : Fan 2/2 : Fan : {} : fan
                     |
                     +-65 (cevFan.179) : Fan 2/3 : Fan : {} : fan
                     |
                     +-66 (cevFan.179) : Fan 2/4 : Fan : {} : fan
                     |
                     +-67 (cevFan.179) : Fan 2/5 : Fan : {} : fan
                     |
                     +-68 (cevFan.179) : Fan 2/6 : Fan : {} : fan
                     |
                     +-69 (cevFan.179) : Fan 2/7 : Fan : {} : fan
                     |
                     +-70 (cevFan.179) : Fan 2/8 : Fan : {} : fan
                     |
                     +-71 (cevFan.179) : Fan 2/9 : Fan : {} : fan
                     |
                     +-72 (cevFan.179) : Fan 2/10 : Fan : {} : fan
                     |
                     \-73 (cevFan.179) : Fan 2/11 : Fan : {} : fan
Line length limited to: <132>
Mib Variables printed : <entPhysicalName entPhysicalDescr entPhysicalModelName
entPhysicalClass>
```

Sample of ENTITY-MIB entPhysicalTable Entries

The samples in this section show how information is stored in the entPhysicalTable. An asset inventory can be performed by examining entPhysicalTable entries.

Note The sample outputs and values that appear throughout this chapter are examples of data that is displayed when using MIBs.

The following is a sample output that shows the ENTITY-MIB entPhysicalTable sample entries for a 8-port Gigabit Ethernet Interface Module card installed in a router chassis, and the IM inserted into the card.

ENTITY-MIB entPhysicalTable Entries

```
eentPhysicalDescr.1050 = 8-port Gigabit Ethernet Interface Module
entPhysicalDescr.1051 = A900-IM8T
entPhysicalDescr.1052 = A900-IM8T
entPhysicalDescr.1053 = A900-IM8T
entPhysicalDescr.1054 = A900-IM8T
entPhysicalDescr.1055 = A900-IM8T
entPhysicalDescr.1056 = A900-IM8T
entPhysicalDescr.1057 = A900-IM8T
entPhysicalDescr.1058 = A900-IM8T
entPhysicalDescr.1067 = subslot 0/3 temperature Sensor 0
entPhysicalDescr.1068 = subslot 0/3 temperature Sensor 1
entPhysicalDescr.1069 = subslot 0/3 temperature Sensor 2
entPhysicalDescr.1070 = subslot 0/3 temperature Sensor 3
entPhysicalDescr.1071 = subslot 0/3 temperature Sensor 4
entPhysicalDescr.1079 = subslot 0/3 voltage Sensor 0
entPhysicalDescr.1080 = subslot 0/3 voltage Sensor 1
```

```
entPhysicalDescr.1081 = subslot 0/3 voltage Sensor 2
entPhysicalDescr.1082 = subslot 0/3 voltage Sensor 3
entPhysicalDescr.1083 = subslot 0/3 voltage Sensor 4
entPhysicalDescr.1084 = subslot 0/3 voltage Sensor 5
....

entPhysicalVendorType.1050 = cevIM8pGeCu
entPhysicalVendorType.1051 = cevPortGe
entPhysicalVendorType.1052 = cevPortGe
entPhysicalVendorType.1053 = cevPortGe
entPhysicalVendorType.1054 = cevPortGe
entPhysicalVendorType.1055 = cevPortGe
entPhysicalVendorType.1056 = cevPortGe
entPhysicalVendorType.1057 = cevPortGe
entPhysicalVendorType.1058 = cevPortGe
entPhysicalVendorType.1067 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1068 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1069 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1070 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1071 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1079 = cevSensorModuleDeviceVoltage
entPhysicalVendorType.1080 = cevSensorModuleDeviceVoltage
entPhysicalVendorType.1081 = cevSensorModuleDeviceVoltage
entPhysicalVendorType.1082 = cevSensorModuleDeviceVoltage
entPhysicalVendorType.1083 = cevSensorModuleDeviceVoltage
entPhysicalVendorType.1084 = cevSensorModuleDeviceVoltage
```

where **entPhysicalVendorType** identifies the unique vendor-specific hardware type of the physical entity.

```
entPhysicalContainedIn.1050 = 7
entPhysicalContainedIn.1051 = 1050
entPhysicalContainedIn.1052 = 1050
entPhysicalContainedIn.1053 = 1050
entPhysicalContainedIn.1054 = 1050
entPhysicalContainedIn.1055 = 1050
entPhysicalContainedIn.1056 = 1050
entPhysicalContainedIn.1057 = 1050
entPhysicalContainedIn.1058 = 1050
entPhysicalContainedIn.1067 = 1050
entPhysicalContainedIn.1068 = 1050
entPhysicalContainedIn.1069 = 1050
entPhysicalContainedIn.1070 = 1050
entPhysicalContainedIn.1071 = 1050
entPhysicalContainedIn.1079 = 1050
entPhysicalContainedIn.1080 = 1050
entPhysicalContainedIn.1081 = 1050
entPhysicalContainedIn.1082 = 1050
entPhysicalContainedIn.1083 = 1050
entPhysicalContainedIn.1084 = 1050
```

where **entPhysicalContainedIn** indicates the entPhysicalIndex of parent entity of the component.

```
entPhysicalClass.1050 = module(9)
entPhysicalClass.1051 = port(10)
entPhysicalClass.1052 = port(10)
entPhysicalClass.1053 = port(10)
entPhysicalClass.1054 = port(10)
entPhysicalClass.1055 = port(10)
entPhysicalClass.1056 = port(10)
entPhysicalClass.1057 = port(10)
entPhysicalClass.1058 = port(10)
```

```
entPhysicalClass.1067 = sensor(8)
entPhysicalClass.1068 = sensor(8)
entPhysicalClass.1069 = sensor(8)
entPhysicalClass.1070 = sensor(8)
entPhysicalClass.1071 = sensor(8)
entPhysicalClass.1079 = sensor(8)
entPhysicalClass.1080 = sensor(8)
entPhysicalClass.1081 = sensor(8)
entPhysicalClass.1082 = sensor(8)
entPhysicalClass.1083 = sensor(8)
entPhysicalClass.1084 = sensor(8)
```

where **entPhysicalClass** indicates the general type of hardware device.

```
entPhysicalParentRelPos.1050 = 0
entPhysicalParentRelPos.1051 = 0
entPhysicalParentRelPos.1052 = 1
entPhysicalParentRelPos.1053 = 2
entPhysicalParentRelPos.1054 = 3
entPhysicalParentRelPos.1055 = 4
entPhysicalParentRelPos.1056 = 5
entPhysicalParentRelPos.1057 = 6
entPhysicalParentRelPos.1058 = 7
entPhysicalParentRelPos.1067 = 0
entPhysicalParentRelPos.1068 = 1
entPhysicalParentRelPos.1069 = 2
entPhysicalParentRelPos.1070 = 3
entPhysicalParentRelPos.1071 = 4
entPhysicalParentRelPos.1079 = 12
entPhysicalParentRelPos.1080 = 13
entPhysicalParentRelPos.1081 = 14
entPhysicalParentRelPos.1082 = 15
entPhysicalParentRelPos.1083 = 16
entPhysicalParentRelPos.1084 = 17
```

where **entPhysicalParentRelPos** indicates the relative position of this child among the other entities.

```
entPhysicalName.1050 = IM subslot 0/3
entPhysicalName.1051 = GigabitEthernet0/3/0
entPhysicalName.1052 = GigabitEthernet0/3/1
entPhysicalName.1053 = GigabitEthernet0/3/2
entPhysicalName.1054 = GigabitEthernet0/3/3
entPhysicalName.1055 = GigabitEthernet0/3/4
entPhysicalName.1056 = GigabitEthernet0/3/5
entPhysicalName.1057 = GigabitEthernet0/3/6
entPhysicalName.1058 = GigabitEthernet0/3/7
entPhysicalName.1067 = subslot 0/3 temperature Sensor 0
entPhysicalName.1068 = subslot 0/3 temperature Sensor 1
entPhysicalName.1069 = subslot 0/3 temperature Sensor 2
entPhysicalName.1070 = subslot 0/3 temperature Sensor 3
entPhysicalName.1071 = subslot 0/3 temperature Sensor 4
entPhysicalName.1079 = subslot 0/3 voltage Sensor 0
entPhysicalName.1080 = subslot 0/3 voltage Sensor 1
entPhysicalName.1081 = subslot 0/3 voltage Sensor 2
entPhysicalName.1082 = subslot 0/3 voltage Sensor 3
entPhysicalName.1083 = subslot 0/3 voltage Sensor 4
entPhysicalName.1084 = subslot 0/3 voltage Sensor 5
```

where **entPhysicalName** provides the textual name of the physical entity.

```
entPhysicalHardwareRev.1050 = V00
```

```
entPhysicalHardwareRev.1051 =
entPhysicalHardwareRev.1052 =
entPhysicalHardwareRev.1053 =
entPhysicalHardwareRev.1054 =
entPhysicalHardwareRev.1055 =
entPhysicalHardwareRev.1056 =
entPhysicalHardwareRev.1057 =
entPhysicalHardwareRev.1058 =
entPhysicalHardwareRev.1067 =
entPhysicalHardwareRev.1068 =
entPhysicalHardwareRev.1069 =
entPhysicalHardwareRev.1070 =
entPhysicalHardwareRev.1071 =
entPhysicalHardwareRev.1079 =
entPhysicalHardwareRev.1080 =
entPhysicalHardwareRev.1081 =
entPhysicalHardwareRev.1082 =
entPhysicalHardwareRev.1083 =
entPhysicalHardwareRev.1084 =
```

where **entPhysicalHardware** provides the vendor-specific hardware revision number (string) for the physical entity.

```
entPhysicalSerialNum.1050 = N/A
entPhysicalSerialNum.1051 =
entPhysicalSerialNum.1052 =
entPhysicalSerialNum.1053 =
entPhysicalSerialNum.1054 =
entPhysicalSerialNum.1055 =
entPhysicalSerialNum.1056 =
entPhysicalSerialNum.1057 =
entPhysicalSerialNum.1058 =
entPhysicalSerialNum.1067 =
entPhysicalSerialNum.1068 =
entPhysicalSerialNum.1069 =
entPhysicalSerialNum.1070 =
entPhysicalSerialNum.1071 =
entPhysicalSerialNum.1079 =
entPhysicalSerialNum.1080 =
entPhysicalSerialNum.1081 =
entPhysicalSerialNum.1082 =
entPhysicalSerialNum.1083 =
entPhysicalSerialNum.1084 =
```

where **entPhysicalSerialNumber** provides the vendor-specific serial number (string) for the physical entity.

```
entPhysicalMfgName.1050 = Cisco Systems Inc
entPhysicalMfgName.1051 =
entPhysicalMfgName.1052 =
entPhysicalMfgName.1053 =
entPhysicalMfgName.1054 =
entPhysicalMfgName.1055 =
entPhysicalMfgName.1056 =
entPhysicalMfgName.1057 =
entPhysicalMfgName.1058 =
entPhysicalMfgName.1067 =
entPhysicalMfgName.1068 =
entPhysicalMfgName.1069 =
entPhysicalMfgName.1070 =
entPhysicalMfgName.1071 =
entPhysicalMfgName.1079 =
```

```
entPhysicalMfgName.1080 =
entPhysicalMfgName.1081 =
entPhysicalMfgName.1082 =
entPhysicalMfgName.1083 =
entPhysicalMfgName.1084 =
```

where **entPhysicalMfgName** provides the name of the manufacturer for the physical component.

```
entPhysicalModelName.1050 = A900-IM8T
entPhysicalModelName.1051 =
entPhysicalModelName.1052 =
entPhysicalModelName.1053 =
entPhysicalModelName.1054 =
entPhysicalModelName.1055 =
entPhysicalModelName.1056 =
entPhysicalModelName.1057 =
entPhysicalModelName.1058 =
entPhysicalModelName.1067 =
entPhysicalModelName.1068 =
entPhysicalModelName.1069 =
entPhysicalModelName.1070 =
entPhysicalModelName.1071 =
entPhysicalModelName.1079 =
entPhysicalModelName.1080 =
entPhysicalModelName.1081 =
entPhysicalModelName.1082 =
entPhysicalModelName.1083 =
entPhysicalModelName.1084 =
```

where **entPhysicalModelName** provides the vendor-specific model name string for the physical component.

```
entPhysicalIsFRU.1050 = true(1)
entPhysicalIsFRU.1051 = false(2)
entPhysicalIsFRU.1052 = false(2)
entPhysicalIsFRU.1053 = false(2)
entPhysicalIsFRU.1054 = false(2)
entPhysicalIsFRU.1055 = false(2)
entPhysicalIsFRU.1056 = false(2)
entPhysicalIsFRU.1057 = false(2)
entPhysicalIsFRU.1058 = false(2)
entPhysicalIsFRU.1067 = false(2)
entPhysicalIsFRU.1068 = false(2)
entPhysicalIsFRU.1069 = false(2)
entPhysicalIsFRU.1070 = false(2)
entPhysicalIsFRU.1071 = false(2)
entPhysicalIsFRU.1079 = false(2)
entPhysicalIsFRU.1080 = false(2)
entPhysicalIsFRU.1081 = false(2)
entPhysicalIsFRU.1082 = false(2)
entPhysicalIsFRU.1083 = false(2)
entPhysicalIsFRU.1084 = false(2)
```

where **entPhysicalIsFRU** indicates whether or not this physical entity is considered a FRU.

Note the following about the sample configuration:

- All chassis slots and IM ports have the same entPhysicalContainedIn value:
  - For chassis slots, entPhysicalContainedIn = 1 (the entPhysicalIndex of the chassis).
  - For IM ports, the entPhysicalContainedIn = 1050 (the entPhysicalIndex of the IM card).
- Each chassis slot and IM card port has a different entPhysicalParentRelPos to show its relative position within the parent object.

Determining the ifIndex Value for a Physical Port

The ENTITY-MIB **entAliasMappingIdentifier** maps a physical port to an interface by mapping the port's entPhysicalIndex to its corresponding ifIndex value in the IF-MIB ifTable. The following sample shows that the physical port whose entPhysicalIndex is 35 is associated with the interface whose ifIndex value is 4. (See the MIB for detailed descriptions of possible MIB values.)

```
entAliasMappingIdentifer.1813.0 = ifIndex.4
```

Monitoring and Configuring FRU Status

View objects in the CISCO-ENTITY-FRU-CONTROL-MIB cefcModuleTable to determine the administrative and operational status of FRUs, such as power supplies and line cards:

- cefcModuleAdminStatus—The administrative state of the FRU. Use cefcModuleAdminStatus to enable or disable the FRU.
- cefcModuleOperStatus—The current operational state of the FRU.

Figure A-1 shows a cefcModuleTable entry for a IM card whose entPhysicalIndex is 1000.

Figure A-1 Sample cefcModuleTable Entry

```
cefcModuleAdminStatus.1000 = enabled(1)
cefcModuleOperStatus.1000 = ok(2)
cefcModuleResetReason.1000 = unknown(1)
cefcModuleStatusLastChangeTime.1000 =
15865
```

See the "FRU Status Changes" section on page A-25 for information about how the router generates notifications to indicate changes in FRU status.

Using ENTITY-ALARM-MIB to Monitor Entity Alarms

CISCO-ENTITY-ALARM-MIB

CISCO-ENTITY-ALARM-MIB supports the monitoring of alarms generated by physical entities contained by the system, including chassis, slots, modules, ports, power supplies, etc. In order to monitor alarms generated by a physical entity, it must be represented by a row in the entPhysicalTable.

For more information on this MIB, refer to CISCO-ENTITY-ALARM-MIB, page 3-24.

Alarm Description Map Table

For each type of entity (represented by entPhysicalVendorType OID), this table contains a mapping between a unique ceAlarmDescrIndex and entPhysicalvendorType OID.

The ceAlarmDescrMapEntry is indexed by the CeAlarmDescrMapEntry.

Note The mapping between the ceAlarmDescrIndex and entPhysicalvendorType OID will exist only if the type of entity supports alarms monitoring, and it is in the device since device boot-up.

The following is a sample output of the alarm description map tables:

```
ptolemy:24> getmany 10.86.0.50 ceAlarmDescrMapTable
ceAlarmDescrVendorType.1 = cevContainerSFP
ceAlarmDescrVendorType.2 = cevContainerSlot
ceAlarmDescrVendorType.3 = cevContainer.246
ceAlarmDescrVendorType.4 = cevContainer.249
ceAlarmDescrVendorType.5 = cevContainer.247
ceAlarmDescrVendorType.6 = cevContainer.248
ceAlarmDescrVendorType.7 = cevSensorModuleDeviceTemp
ceAlarmDescrVendorType.8 = cevSensorModuleDeviceVoltage
ceAlarmDescrVendorType.9 = cevSensorModuleDeviceCurrent
ceAlarmDescrVendorType.10 = cevSensor
ceAlarmDescrVendorType.11 = cevModule.87.1
ceAlarmDescrVendorType.12 = cevPortUSB
ceAlarmDescrVendorType.13 = cevPortGe
ceAlarmDescrVendorType.14 = cevFan.178
ceAlarmDescrVendorType.15 = cevModuleCommonCards.334
ceAlarmDescrVendorType.16 = cevModuleCommonCards.336
```

The temperature sensor in ASR903 modules (RSP and PEM) contain cevSensorModuleDeviceTemp as entPhysicalvendorType OID. From the sample output, the index (ceAlarmDescrIndex) 7 is mapped to cevSensorModuleDeviceTemp, and the index 14 is mapped to the ASR 903 FAN module, which has cevFan.178 as entity physical vendor type OID.

Note The generic vendor OID, cevSenor, is used in case the Cisco ASR 903 SNMP agent is not able to determine the sensor type.

Alarm Description Table

The Alarm Description Table contains a description for each alarm type, defined by each vendor type employed by the system. Each alarm description entry (ceAlarmDescrEntry) is indexed by ceAlarmDescrIndex and ceAlarmDescrAlarmType.

The following is the sample output for all alarm types defined for all temperature types of entities in the Cisco ASR 903 modules. The index 9 is obtained from the ceAlarmDescrMapTable in the previous section:

```
ptolemy:26> getmany 10.86.0.50 ceAlarmDescrTable | grep "\.9\."
ceAlarmDescrSeverity.9.0 = 1
ceAlarmDescrSeverity.9.1 = 1
ceAlarmDescrSeverity.9.2 = 1
ceAlarmDescrSeverity.9.3 = 2
ceAlarmDescrSeverity.9.4 = 3
ceAlarmDescrSeverity.9.5 = 1
ceAlarmDescrSeverity.9.6 = 1
ceAlarmDescrSeverity.9.7 = 2
ceAlarmDescrSeverity.9.8 = 3
ceAlarmDescrText.9.0 = Faulty Ampere Sensor
ceAlarmDescrText.9.1 = Ampere Above Normal (Shutdown)
ceAlarmDescrText.9.2 = Ampere Above Normal
ceAlarmDescrText.9.3 = Ampere Above Normal
ceAlarmDescrText.9.4 = Ampere Above Normal
ceAlarmDescrText.9.5 = Ampere Below Normal (Shutdown)
ceAlarmDescrText.9.6 = Ampere Below Normal
ceAlarmDescrText.9.7 = Ampere Below Normal
ceAlarmDescrText.9.8 = Ampere Below Normal
```

Refer to the Bellcore Technical Reference TR-NWT-000474 Issue 4, December 1993, OTGR Section 4. Network Maintenance: Alarm and Control - Network Element. The severity is defined as follows:

- critical(1)
- major(2)
- minor(3)
- info(4)

The following is the list of alarms defined for the sensor:

```
Alarm type 1 is for crossing the shutdow threshold (above normal range).
Alarm type 2 is for crossing the critical threshold (above normal range).
Alarm type 3 is for crossing the major threshold (above normal range).
Alarm type 4 is for crossing the minor threshold (above normal range).
Alarm type 5 is for crossing the shutdow threshold (below normal range).
Alarm type 6 is for crossing the critical threshold (below normal range).
Alarm type 7 is for crossing the major threshold (below normal range).
Alarm type 8 is for crossing the minor threshold (below normal range).
```

These alarm types are defined for all sensor physical entity type. The only difference is that different sensor physical type have different ceAlarmDescrText. The temperature sensor has "TEMP" and the voltage sensor has "Volt" in the alarm description text.

The following is the sample output of all alarm types. It is defined for the Cisco ASR903 Router fan module which has cevFan.178 as vendor type OID and is mapped to the ceAlarmDescrIndex

```
ptolemy:27> getmany 10.86.0.50 ceAlarmDescrTable | grep "\.14\."
ceAlarmDescrSeverity.14.0 = 1
ceAlarmDescrSeverity.14.1 = 1
ceAlarmDescrSeverity.14.2 = 1
ceAlarmDescrSeverity.14.3 = 2
ceAlarmDescrSeverity.14.4 = 2
ceAlarmDescrSeverity.14.5 = 2
ceAlarmDescrSeverity.14.6 = 2
ceAlarmDescrSeverity.14.7 = 2
ceAlarmDescrSeverity.14.8 = 2
```

```
ceAlarmDescrSeverity.14.9 = 2
ceAlarmDescrSeverity.14.10 = 2
ceAlarmDescrSeverity.14.11 = 2
ceAlarmDescrSeverity.14.12 = 2
ceAlarmDescrSeverity.14.13 = 2
ceAlarmDescrSeverity.14.14 = 2
ceAlarmDescrText.14.0 = Fan Tray/Module Failure
ceAlarmDescrText.14.1 = All Fans Failed
ceAlarmDescrText.14.2 = Multiple Fan Failures
ceAlarmDescrText.14.3 = Fan 0 Failure
ceAlarmDescrText.14.4 = Fan 1 Failure
ceAlarmDescrText.14.5 = Fan 2 Failure
ceAlarmDescrText.14.6 = Fan 3 Failure
ceAlarmDescrText.14.7 = Fan 4 Failure
ceAlarmDescrText.14.8 = Fan 5 Failure
ceAlarmDescrText.14.9 = Fan 6 Failure
ceAlarmDescrText.14.10 = Fan 7 Failure
ceAlarmDescrText.14.11 = Fan 8 Failure
ceAlarmDescrText.14.12 = Fan 9 Failure
ceAlarmDescrText.14.13 = Fan 10 Failure
ceAlarmDescrText.14.14 = Fan 11 Failure
```

Alarm Table

The Alarm Table specifies alarm control and status information related to each physical entity contained by the system. The table includes the alarms currently being asserted by each physical entity that is capable of generating alarms. Each physical entity in entity physical table that is capable of generating alarms has an entry in this table.The alarm entry (ceAlarmEntry) is indexed by the entity physical index (entPhysicalIndex). The following is a list of MIB objects in the alarm entry:

- **ceAlarmFilterProfile**
  The alarm filter profile object contains an integer value that uniquely identifies an alarm filter profile associated with the corresponding physical entity. An alarm filter profile controls which alarm types the agent will monitor and signal for the corresponding physical entity. The default value of this object is 0, the agent monitors and signals all alarms associated with the corresponding physical entity.
- **ceAlarmSeverity**
  This object specifies the highest severity alarm currently being asserted by the corresponding physical entity.
  A value of '0' indicates that the corresponding physical entity is not currently asserting any alarms.
- **ceAlarmList**
  This object specifies those alarms currently being asserted by the corresponding physical entity. If an alarm is being asserted by the physical entity, then the corresponding bit in the alarm list is set to a one. The alarm list is defined as octet string and its size ranges from 0 to 32.
  - If the physical entity is not currently asserting any alarms, then the list will have a length of zero, otherwise it will have a length of 32.
  - An OCTET STRING represents an alarm list, in which each bit represents an alarm type:

octet 1:

```
7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+
| |
+-+-+-+-+-+-+-+-+
| | | | | | | |
```

```
| | | | | | | +- Alarm type 0
| | | | | | +--- Alarm type 1
| | | | | +----- Alarm type 2
| | | | +------- Alarm type 3
| | | +--------- Alarm type 4
| | +----------- Alarm type 5
| +------------- Alarm type 6
+--------------- Alarm type 7
```

octet 2:

```
7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+
| |
+-+-+-+-+-+-+-+-+
| | | | | | | |
| | | | | | | +- Alarm type 8
| | | | | | +--- Alarm type 9
| | | | | +----- Alarm type 10
| | | | +------- Alarm type 11
| | | +--------- Alarm type 12
| | +----------- Alarm type 13
| +------------- Alarm type 14
+--------------- Alarm type 15
```

octet xx

```
7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+
| |
+-+-+-+-+-+-+-+-+
| | | | | | | |
| | | | | | | +- Alarm type 248
| | | | | | +--- Alarm type 249
| | | | | +----- Alarm type 250
| | | | +------- Alarm type 251
| | | +--------- Alarm type 252
| | +----------- Alarm type 253
| +------------- Alarm type 254
+--------------- Alarm type 255
```

The entity physical table (entPhysicalTable in ENTITY-MIB), indicates that the Cisco ASR903 Router AC power supply in power supply bay 0 has 4 as entPhysicalIndex .

The following is the sample output of the alarm list for the power supply in PS bay 0:

```
ptolemy-248->getone -v2c 9.0.0.56 public ceAlarmList.4
ceAlarmList.10 =
01 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00
00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00
```

octet 1: 09

```
7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+
0 0 0 0 1 0 0 1
+-+-+-+-+-+-+-+-+
| | | | | | | |
```

```
| | | | | | | +- Alarm type 0
| | | | | | +--- Alarm type 1
| | | | | +----- Alarm type 2
| | | | +------- Alarm type 3
| | | +--------- Alarm type 4
| | +----------- Alarm type 5
| +------------- Alarm type 6
+--------------- Alarm type 7
```

From the sample output in the Alarm Description Table section and the alarm mapping table, the ASR903 AC power supply in the bay 0 has the following alarms asserted:

Alarm type 0 : Power Supply Failure

Alarm type 3 : Fan 0 Failure

The following is the output of the **show facility-alarm status** command; it displays all alarms currently asserted in the device:

```
System Totals  Critical: 11  Major: 0  Minor: 0

Source              Severity      Description [Index]
------              --------      -------------------
Power Supply Bay 0          CRITICAL      Power Supply/FAN Module Missing [0]
TenGigabitEthernet0/1/0     CRITICAL      Physical Port Link Down [35]
TenGigabitEthernet0/2/0     CRITICAL      Physical Port Link Down [35]
xcvr container 0/4/0        CRITICAL      Transceiver Missing - Link Down [1]
GigabitEthernet0/4/4        CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/4/5        CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/4/6        CRITICAL      Physical Port Link Down [1]
xcvr container 0/5/0        CRITICAL      Transceiver Missing - Link Down [1]
GigabitEthernet0/5/1        CRITICAL      Physical Port Link Down [1]
xcvr container 0/5/2        CRITICAL      Transceiver Missing - Link Down [1]
GigabitEthernet0/5/3        CRITICAL      Physical Port Link Down [1]
```

Alarm History Table

The Alarm History Table, ceAlarmHistTable, contains history of alarms both asserted and cleared generated by the agent. The ceAlarmHistTableSize is used to control the size of the alarm history table. A value of 0 prevents any history from being retained in this table. If the capacity of the ceAlarmHistTable has reached the value specified by this object, then the agent deletes the oldest entity in order to accommodate a new entry.

The ceAlarmHistLastIndex object contains the last index corresponding to the last entry added to the table by the snmp agent in the device. If the management client uses notifications listed in the Appendix A, “Alarm Notifications” defined in CISCO-ENTITY-ALARM-MIB module, then it can poll this object to determine whether it has missed a notification sent by the agent.

The following is a list of MIB objects defined in the ceAlarmHistEntry, which is indexed by the ceAlarmHistIndex:

- **ceAlarmHistIndex**
  This is an integer value uniquely identifying the entry in the table. The value of this object starts at '1' and monotonically increases for each alarm (asserted or cleared) added to the alarm history table. If the value of this object is '4294967295', it will be reset to '1', upon monitoring the next alarm condition transition.
- **ceAlarmHistType**
  This object indicates that the entry is added as a result of of an alarm being asserted or cleared.

- **ceAlarmHistEntPhysicalIndex**
  This object contains the entPhysicalIndex of the physical entity that generated the alarm.
- **ceAlarmHistAlarmType**
  This object specifies the type of alarm generated.
- **ceAlarmHistSeverity**
  This object specifies the severity of the alarm generated.
- **ceAlarmHistTimeStamp**
  This object specifies the value of the sysUpTime object at the time the alarm is generated.

Example A-3 Displaying Sample Output for the Alarm History

```
ptolemy:33> getnext 10.86.0.50 ceAlarmHistory
ceAlarmHistTableSize.0 = 200 → the size of alarm history table
ptolemy:34> getnext 10.86.0.50 ceAlarmHistTableSize.0
ceAlarmHistLastIndex.0 = 21 → the index for the last alarm added
```

Example A-4 Displaying the Last Alarm Action (asserted or cleared) Added to the Alarm History Table

```
ptolemy:37> getmany 10.86.0.50 ceAlarmHistTable | grep "\.99"
ceAlarmHistType.99 = cleared(2)
ceAlarmHistEntPhysicalIndex.99 = 800
ceAlarmHistAlarmType.99 = 0
ceAlarmHistSeverity.99 = major(2)
ceAlarmHistTimeStamp.99 = 20033972
```

At this point, the EMS application should already have all information regarding the physical entity and the entity alarm type defined for the physical entity.

Example A-5 Displaying the Physical Entity with Value 51 as entPhysicalIndex

```
entPhysicalDescr.51 = ASR 903 FAN Tray
entPhysicalVendorType.51 = cevFan.178
entPhysicalContainedIn.51 = 50
entPhysicalClass.51 = fan(7)
entPhysicalParentRelPos.51 = 0
entPhysicalName.51 = Fan Tray
entPhysicalHardwareRev.51 = V00
entPhysicalFirmwareRev.51 =
entPhysicalSoftwareRev.51 =
entPhysicalSerialNum.51 =
entPhysicalMfgName.51 = Cisco Systems Inc
entPhysicalModelName.51 = A903-FAN
```

Example A-6 Displaying the Alarm Type Defined for cevFan.178

```
ceAlarmDescrSeverity.18.0 = 1
ceAlarmDescrSeverity.18.1 = 1
ceAlarmDescrSeverity.18.2 = 1
ceAlarmDescrSeverity.18.3 = 2
ceAlarmDescrSeverity.18.4 = 2
ceAlarmDescrSeverity.18.5 = 2
ceAlarmDescrSeverity.18.6 = 2
ceAlarmDescrSeverity.18.7 = 2
ceAlarmDescrSeverity.18.8 = 2
ceAlarmDescrSeverity.18.9 = 2
ceAlarmDescrSeverity.18.10 = 2
```

```
ceAlarmDescrSeverity.18.11 = 2
ceAlarmDescrSeverity.18.12 = 2
ceAlarmDescrSeverity.18.13 = 2
ceAlarmDescrSeverity.18.14 = 2
ceAlarmDescrText.18.0 = Fan Tray/Module Failure
ceAlarmDescrText.18.1 = All Fans Failed
ceAlarmDescrText.18.2 = Multiple Fan Failures
ceAlarmDescrText.18.3 = Fan 0 Failure
ceAlarmDescrText.18.4 = Fan 1 Failure
ceAlarmDescrText.18.5 = Fan 2 Failure
ceAlarmDescrText.18.6 = Fan 3 Failure
ceAlarmDescrText.18.7 = Fan 4 Failure
ceAlarmDescrText.18.8 = Fan 5 Failure
ceAlarmDescrText.18.9 = Fan 6 Failure
ceAlarmDescrText.18.10 = Fan 7 Failure
ceAlarmDescrText.18.11 = Fan 8 Failure
ceAlarmDescrText.18.12 = Fan 9 Failure
ceAlarmDescrText.18.13 = Fan 10 Failure
ceAlarmDescrText.18.14 = Fan 11 Failure
```

Alarm Notifications

CISCO-ENTITY-ALARM-MIB supports the alarm asserted (ceAlarmAsserted) and alarm cleared (ceAlarmCleared) notifications. The notification can be enabled by setting the ceAlarmNotifiesEnable object through the snmp SET. The ceAlarmNotifiesEnable contains the severity level of the alarms notification or the value 0:

```
severity 1: critical       Service affecting Condition
severity 2: major          Immediate action needed
severity 3: minor          Minor warning conditions
severity 4: informational  Informational messages
```

The severity 4 will enable notification for all severity level.

The severity 3 will enable notifications for severity 1, 2, and 3.

The severity 2 will enable notifications for severity 1 and 2.

The severity 1 will enable notifications for severity 1 only.

The value of 0 will disable the alarm notification.

The alarm notification can be enabled or disabled via the CLI command. Use the "NO" form to disable the alarm notification:

```
snmp-server enable traps alarm [critical, major, minor, information]
no snmp-server enable traps alarm [critical, major, minor, information]
```

The alarm notification contains exactly the same information described in alarm history entry. Refer to the Alarm History Table Section for the MIB objects and to interpret the alarm notifications received.

Example A-7 Displaying the Sample Notification Received

```
sysUpTime.0 = 161726
 snmpTrapOID.0 = ceAlarmAsserted
 ceAlarmHistEntPhysicalIndex.103 = 800
 ceAlarmHistAlarmType.103 = 0
 ceAlarmHistSeverity.103 = 2
 ceAlarmHistTimeStamp.103 = 161725
 ceAlarmDescrText.17.0 = Unknown state

sysUpTime.0 = 161728
```

```
 snmpTrapOID.0 = ceAlarmCleared
 ceAlarmHistEntPhysicalIndex.104 = 801
 ceAlarmHistAlarmType.104 = 5
 ceAlarmHistSeverity.104 = 3
 ceAlarmHistTimeStamp.104 = 161725
 ceAlarmDescrText.18.5 = Receiver has loss of signal

sysUpTime.0 = 161729
 snmpTrapOID.0 = ceAlarmCleared
 ceAlarmHistEntPhysicalIndex.105 = 801
 ceAlarmHistAlarmType.105 = 12
 ceAlarmHistSeverity.105 = 3
 ceAlarmHistTimeStamp.105 = 161725
 ceAlarmDescrText.18.12 = Ds1 Physical Port Link Down
```

Generating SNMP Notifications

This section provides information about the SNMP notifications generated in response to events and conditions on the router, and describes how to identify the hosts that are to receive notifications.

- Identifying Hosts to Receive Notifications
- Configuration Changes
- FRU Status Changes

Identifying Hosts to Receive Notifications

You can use the CLI or SNMP to identify hosts to receive SNMP notifications and to specify the types of notifications they are to receive (notifications or informs). For CLI instructions, see the "Monitoring Notifications" section on page 4-1. To use SNMP to configure this information, use the following MIB objects:

Use SNMP-NOTIFICATION-MIB objects, including the following, to select target hosts and specify the types of notifications to generate for those hosts:

- snmpNotifyTable—Contains objects to select hosts and notification types:
  - snmpNotifyTag is an arbitrary octet string (a tag value) used to identify the hosts to receive SNMP notifications. Information about target hosts is defined in the snmpTargetAddrTable (SNMP-TARGET-MIB), and each host has one or more tag values associated with it. If a host in snmpTargetAddrTable has a tag value that matches this snmpNotifyTag value, the host is selected to receive the types of notifications specified by snmpNotifyType.
  - snmpNotifyType is the type of SNMP notification to send: notification(1) or inform(2).
- snmpNotifyFilterProfileTable and snmpNotifyFilterTable—Use objects in these tables to create notification filters to limit the types of notifications sent to target hosts.

Use SNMP-TARGET-MIB objects to configure information about the hosts to receive notifications:

- snmpTargetAddrTable—Transport addresses of hosts to receive SNMP notifications. Each entry provides information about a host address, including a list of tag values:
  - snmpTargetAddrTagList—A set of tag values associated with the host address. If a host's tag value matches snmpNotifyTag, the host is selected to receive the types of notifications defined by snmpNotifyType.
- snmpTargetParamsTable—SNMP parameters to use when generating SNMP notifications.

Use the notification enable objects in appropriate MIBs to enable and disable specific SNMP notifications. For example, to generate mplsLdpSessionUp or mplsLdpSessionDown notifications, the MPLS-LDP-MIB object mplsLdpSessionUpDownTrapEnable must be set to enabled(1).

Configuration Changes

If entity notifications are enabled, the router generates an entConfigChange notification (ENTITY-MIB) when the information in any of the following tables changes (which indicates a change to the router configuration):

- entPhysicalTable
- entAliasMappingTable
- entPhysicalContainsTable

Note A management application that tracks configuration changes checks the value of the entLastChangeTime object to detect any entConfigChange notifications that were missed as a result of throttling or transmission loss.

Enabling notifications for Configuration Changes

To configure the router to generate an entConfigChange notification each time its configuration changes, enter the following command from the CLI. Use the **no** form of the command to disable the notifications.

```
Router(config)# snmp-server enable traps entity
Router(config)# no snmp-server enable traps entity
```

FRU Status Changes

If FRU notifications are enabled, the router generates the following notifications in response to changes in the status of an FRU:

- cefcModuleStatusChange—The operational status (cefcModuleOperStatus) of an FRU changes.
- cefcFRUInserted—An FRU is inserted in the chassis. The notification indicates the entPhysicalIndex of the FRU and the container it was inserted in.
- cefcFRURemoved—An FRU is removed from the chassis. The notification indicates the entPhysicalIndex of the FRU and the container it was removed from.

Note See the CISCO-ENTITY-FRU-CONTROL-MIB for more information about these notifications.

Enabling FRU Notifications

To configure the router to generate notifications for FRU events, enter the following command from the CLI. Use the **no** form of the command to disable the notifications.

```
Router(config)# snmp-server enable traps fru-ctrl
Router(config)# no snmp-server enable traps fru-ctrl
```

To enable FRU notifications through SNMP, set cefcMIBEnableStatusNotification to true(1). Disable the notifications by setting cefcMIBEnableStatusNotification to false(2).

Monitoring Router Interfaces

This section provides information about how to monitor the status of router interfaces to see if there is a problem or a condition that might affect service on the interface. To determine if an interface is Down or experiencing problems, you can:

Check the Interface's Operational and Administrative Status

To check the status of an interface, view the following IF-MIB objects for the interface:

- ifAdminStatus—The administratively configured (desired) state of an interface. Use ifAdminStatus to enable or disable the interface.
- ifOperStatus—The current operational state of an interface.

Monitor linkDown and linkUp Notifications

To determine if an interface has failed, you can monitor linkDown and linkUp notifications for the interface. See the "Enabling Interface linkUp/linkDown Notifications" section on page A-26 for instructions on how to enable these notifications.

- linkDown—Indicates that an interface failed or is about to fail.
- linkUp—Indicates that an interface is no longer in the Down state.

Enabling Interface linkUp/linkDown Notifications

To configure SNMP to send a notification when a router interface changes state to Up (ready) or Down (not ready), perform the following steps to enable linkUp and linkDown notifications:

Step 1 Issue the following CLI command to enable linkUp and linkDown notifications for most, but not necessarily all, interfaces:

```
Router(config)# snmp-server enable traps snmp linkdown linkup
```

Step 2 View the setting of the ifLinkUpDownTrapEnable object (IF-MIB ifXTable) for each interface to determine if linkUp and linkDown notifications are enabled or disabled for that interface.

Step 3 To enable linkUp and linkDown notifications on an interface, set ifLinkUpDownTrapEnable to enabled(1). To configure the router to send linkDown notifications only for the lowest layer of an interface, see the "SNMP Notification Filtering for linkDown Notifications" section on page A-27.

Step 4 To enable the Internet Engineering Task Force (IETF) standard for linkUp and linkDown notifications, issue the following command. (The IETF standard is based on RFC 2233.)

```
Router(config)# snmp-server trap link ietf
```

Step 5 To disable notifications, use the **no** form of the appropriate command.

SNMP Notification Filtering for linkDown Notifications

Use the SNMP notification filtering feature to filter linkDown notifications so that SNMP sends a linkDown notification only if the main interface goes down. If an interfaces goes down, all of its subinterfaces go down, which results in numerous linkDown notifications for each subinterface. This feature filters out those subinterface notifications.

This feature is turned off by default. To enable the SNMP notification filtering feature, issue the following CLI command. Use the **no** form of the command to disable the feature.

```
[no] snmp ifmib trap throttle
```

Billing Customers for Traffic

This section describes how to use SNMP interface counters to determine the amount to bill customers for traffic.

Input and Output Interface Counts

The router maintains information about the number of packets and bytes that are received on an input interface and transmitted on an output interface.

For detailed constraints about IF-MIB counter support, see the "IF-MIB (RFC 2863)" section on page 3-61.

Read the following important information about the IF-MIB counter support:

- Unless noted, all IF-MIB counters are supported on Cisco ASR 903 Series Router interfaces.
- For IF-MIB high capacity counter support, we conform to the RFC 2863 standard. The RFC 2863 standard states that for interfaces that operate:
  - At 20 million bits per second or less, 32-bit byte and packet counters *must* be supported.
  - Faster than 20 million bits per second and slower than 650,000,000 bits per second, 32-bit packet counters and 64-bit octet counters *must* be supported.
  - At 650,000,000 bits per second or faster, 64-bit packet counters *and* 64-bit octet counters *must* be supported.

Using IF-MIB Counters

This section describes the IF-MIB counters and how you can use them on various interfaces and subinterfaces. The subinterface counters are specific to the protocols. This section addresses the IF-MIB counters for ATM interfaces.

The IF-MIB counters are defined with respect to lower and upper layers:

- ifInDiscards—The number of inbound packets which were discarded, even though no errors were detected to prevent their being deliverable to a higher-layer protocol. One reason for discarding such a packet could be to free up buffer space.
- IfInErrors—The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol for packet-oriented interfaces.

- ifInUnknownProtos—The number of packets received through the interface which were discarded because of an unknown or unsupported protocol for packet-oriented interfaces.
- ifOutDiscards—The number of outbound packets which were discarded even though no errors were detected to prevent their being transmitted. One reason for discarding such a packet is to free up buffer space.
- ififOutErrors—The number of outbound packets that could not be transmitted because of errors for packet-oriented interfaces.

The logical flow for counters works as follows:

1. When a packet arrives on an interface, check for the following:
   a. Error in packet—If any errors are detected, increment ifInErrors and drop the packet.
   b. Protocol errors—If any errors are detected, increment ifInUnknownProtos and drop the packet.
   c. Resources (buffers)—If unable to get resources, increment ifInDiscards and drop the packet.
   d. Increment ifInUcastPkts/ ifInNUcastPkts and process the packet (At this point, increment the ifInOctets with the size of packet).
2. When a packet is to be sent out of an interface:
   a. Increment ifOutUcasePkts/ ifOutNUcastPkts (Here we also increment ifOutOctets with the size of packet).
   b. Check for error in packet and if there are any errors in packet, increment ifOutErrors and drop the packet.
   c. Check for resources (buffers) and if you cannot get resources then increment ifOutDiscards and drop packet.

This following output is an example IF-MIB entries:

IfXEntry ::=

```
SEQUENCE {
    ifName                  DisplayString,
    ifInMulticastPkts       Counter32,
    ifInBroadcastPkts       Counter32,
    ifOutMulticastPkts      Counter32,
    ifOutBroadcastPkts      Counter32,
    ifHCInOctets            Counter64,
    ifHCInUcastPkts         Counter64,
    ifHCInMulticastPkts     Counter64,
    ifHCInBroadcastPkts     Counter64,
    ifHCOutOctets           Counter64,
    ifHCOutUcastPkts        Counter64,
    ifHCOutMulticastPkts    Counter64,
    ifHCOutBroadcastPkts    Counter64,
    ifLinkUpDownTrapEnable  INTEGER,
    ifHighSpeed             Gauge32,
    ifPromiscuousMode       TruthValue,
    ifConnectorPresent      TruthValue,
    ifAlias                 DisplayString,
    ifCounterDiscontinuityTime TimeStamp
```

Sample Counters

The high capacity counters are 64-bit versions of the basic ifTable counters. They have the same basic semantics as their 32-bit counterparts; their syntax is extended to 64 bits.

Table A-1 lists capacity counter object identifiers (OIDs).

Table A-1 Capacity Counters Object Identifiers

Name	Object Identifier (OID)
ifHCInOctets	::= { ifXEntry 6 }
ifHCInUcastPkts	::= { ifXEntry 7 }
ifHCInMulticastPkts	::= { ifXEntry 8 }
ifHCInBroadcastPkts	::= { ifXEntry 9 }
ifHCOutOctets	::= { ifXEntry 10 }
ifHCOutUcastPkts	::= { ifXEntry 11 }
ifHCOutMulticastPkts	::= { ifXEntry 12 }
ifHCOutBroadcastPkts	::= { ifXEntry 13 }
ifLinkUpDownTrapEnable	::= { ifXEntry 14 }
ifHighSpeed	::= { ifXEntry 15 }
ifPromiscuousMode	::= { ifXEntry 16 }
ifConnectorPresent	::= { ifXEntry 17 }
ifAlias	::= { ifXEntry 18 }
ifCounterDiscontinuityTime	::= { ifXEntry 19 }

Related Information and Useful Links

The following URLs provide access to helpful information about Cisco IF-MIB counters:

- Frequently asked questions about SNMP counters:

  http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a00800b69ac.shtml

- Access Cisco IOS XE MIB Tools from the following URL:

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

Overview of Interface Module

An Interface Module (IM) is a type of port adapter that inserts into a subslot to provide network connectivity and increased interface port density. The IM helps in providing services related to VPNs, pseudowires, and so on.

The different types of IM cards supported are:

- A900-IMA8S (8-port Gigabit Ethernet Interface Module using SFPs)
- A900-IM8T (8-port Gigabit Ethernet Interface Module with RJ-45 connectors)
- A900-IMA16D (16 port T1/E1 Interface Module)
- A900-IM1X (Ten Gigabit Ethernet Interface Module)

Displaying the Hardware Type

These commands in the Cisco ASR 903 Series Router help to display the hardware details:

- **show platform**

```
Router# show platform

Chassis type: ASR-903
Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0/1 A900-IM8T ok 3d06h
0/2 A900-IMA16D ok 23:21:45
0/3 A900-IM8T ok 3d06h
R0 A900-RSP1A-55 ok, active 3d07h
F0 ok, active 3d07h
P0 Unknown ps, fail never
P1 Unknown ps, fail never
P2 A903-FAN ok 3d07h

Slot CPLD Version Firmware Version
--------- ------------------- ----------------------------------------
R0 11070719 12.2(20110714:143033) [ashohegd-ROMM...
F0 11070719 12.2(20110714:143033) [ashohegd-ROMM...
```

- **show hardware module subslot**

```
Router# show hardware-module
Router# sh hw-module subslot 0/3 ?
entity entity MIB details - not intended for production use
fpd Show Field Programmable Devices (FPD) information
oir Show oir summary
sensors Environmental sensor summary
subblock subblock details - not intended for production use
tech-support Show subslot information for Tech-Support


Router# show hardware-module subslot 0/1 entity
WARNING: This command is not intended for production use and should only be used under the
supervision of Cisco Systems technical support personnel.

Entity state for SPA in subslot 0/1
SPA type:                  (0x73D) 8xGE IM
last spa type:             (0x73D) 8xGE IM
oper_status:               (1) ok
card status:               (2) full
last trap: spa type:       (0x73D) 8xGE IM
last trap: oper status:    (1) ok
last_spa_env_get_ok:       false
last_spa_env_read_time:    (0) 40455228 msecs ago
resync_reqd:               false
resync_count:              0

SPA physical index:        550
SPA container index:       5

SPA has no transceiver subblock
non-zero port indices:
port 0 has index 551
port 1 has index 552
port 2 has index 553
port 3 has index 554
port 4 has index 555
port 5 has index 556
```

```
port 6 has index 557
port 7 has index 558

non-zero SPA temp sensors:
sensor 0 has index 567
sensor 1 has index 568
sensor 2 has index 569
sensor 3 has index 570
sensor 4 has index 571

non-zero SPA volt sensors:
sensor 0 has index 579
sensor 1 has index 580
sensor 2 has index 581
sensor 3 has index 582
sensor 4 has index 583
sensor 5 has index 584
```

GLOSSARY

B

Bandwidth — The difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.

Broadcast storm — Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs.

C

CANA — Cisco Assigned Numbers Authority. The central clearing house for allocation of unique names and numbers that are embedded in Cisco software.

CLI — Command Line Interface

CNEM — Consistent Network Element Manageability

Columnar object — One type of managed object that 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).

Community name — Defines an access environment for a group of NMSs. NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

Critical alarm severity type — Indicates a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week. For example, online insertion and removal of line cards or loss of signal failure when a physical port link is down.

CWDM — Coarse Wavelength Division Multiplexing

D

dBm — Decibel (milliwatts). 10 * log10 (power in milliwatts). For example, 2 milliwatts is 10 * log10 (2) = 10 * 0.3010 = 3.01 dBm

DOM — Digital Optical Monitoring

Display string — A printable ASCII string. It is typically a name or description. For example, the variable netConfigName provides the name of the network configuration file for a device.

DS0 Digital signal level 0. Framing specification used in transmitting digital signals at 64 Kbps. Twenty-four DS0s equal one DS1.

DS1 Digital signal level 1. Framing specification used in transmitting digital signals at 1.544 Mbps on a T1 facility.

DS3 Digital signal level 3. Framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility.

DWDM Dense Wave Division Multiplexing

E

EHSA Enhanced High System Availability.

EMS Element Management System. An EMS manages a specific portion of the network. For example the SunNet Manager, an SNMP management application, is used to manage SNMP manageable elements. Element Managers may manage asynchronous lines, multiplexers, PABX's, proprietary systems or an application.

Encapsulation The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

F

FRU Field Replaceable Unit. Term applied to the Cisco 6400 components that can be replaced in the field, including the NLC, NSP, NRP, and PEM units, plus the blower fans.

Forwarding Process of sending a frame toward its ultimate destination by way of an internetworking device.

Frame Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment are also used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

G

Gb gigabit

GBIC Gigabit Interface Converter —An optical transceiver (transmitter and receiver) housed in a small (30 mm x 65 mm), hot-pluggable, subenclosure. A GBIC converts electric currents (digital highs and lows) to optical signals and optical signals to digital electric currents.

Gbps gigabits per second

GB gigabyte

GBps gigabytes per second

10GE 10 Gigabit per second Ethernet

H

HSRP Hot Standby Routing Protocol. Protocol used among a group of routers for selecting an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met.)

I

IEEE 802.2 IEEE LAN protocol that specifies an implementation of the LLC sublayer of the data link layer. IEEE 802.2 handles errors, framing, flow control, and the network layer (Layer 3) service interface. Used in IEEE 802.3 and IEEE 802.5 LANs. See also IEEE 802.3 and IEEE 802.5.

IEEE 802.3 IEEE LAN protocol that specifies an implementation of the physical layer and the MAC sublayer of the data link layer. IEEE 802.3 uses CSMA/CD access at a variety of speeds over a variety of physical media. Extensions to the IEEE 802.3 standard specify implementations for Fast Ethernet.

IEEE 802.5 IEEE LAN protocol that specifies an implementation of the physical layer and MAC sublayer of the data link layer. IEEE 802.5 uses token passing access at 4 or 16 Mbps over STP cabling and is similar to IBM Token Ring. See also Token Ring.

IETF The Internet Engineering Task Force

Info Notification about a condition that could lead to an impending problem or notification of an event that improves operation.

Informs Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

ifIndex Each row of the interfaces table has an associated number, called an ifIndex. You use the ifIndex number to get a specific instance of an interfaces group object. For example, ifInNUcastPkts.1 would find you the number of broadcast packets received on interface number one. You can then find the description of interface number one by looking at the object which holds the interface description (from MIB-II) ifDescr.

Integer A numeric value that can be an actual number. For example, the number of lost IP packets on an interface. It also can be a number that represents a nonnumeric value. For example, the variable tsLineType returns the type of terminal services line to the SNMP manager.

Interface counters Interface management over SNMP is based on two tables: ifTable and its extension, ifXTable described in RFC1213/RFC2233. Interfaces can have several layers, depending on the media, and each sub-layer is represented by a separate row in the table. The relationship between the higher layer and lower layers is described in the ifStackTable.

The ifTable defines 32-bit counters for inbound and outbound octets (ifInOctets / ifOutOctets), packets (ifInUcastPkts / ifOutUcastPkts, ifInNUcastPkts / ifOutNUcastPkts), errors, and discards.

The ifXTable provides similar 64-bit counters, also called high capacity (HC) counters: ifHCInOctets / ifHCOutOctets, and ifHCInUcastPkts / ifHCOutUcastPkts.

Internetwork Collection of networks interconnected by routers and other devices that functions as a single network. Sometimes called an internet, which is not to be confused with the Internet.

Interoperability Ability of computing equipment manufactured by different vendors to communicate with one another successfully over a network.

IP Address The variable hostConfigAddr indicates the IP address of the host that provided the host configuration file for a device.

J

No terms

K

Keepalive message Message sent by one network device to inform another network device that the virtual circuit between the two is still active.

L

Label A short, fixed-length identifier that is used to determine the forwarding of a packet.

LDP Label Distribution Protocol.

LR Long Reach.

LSR Label Switching Router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

LSP Label Switched Path.

LX/LH Long wavelength/long haul

M

Major alarm severity type Used for hardware or software conditions. Indicates a serious disruption of service or the malfunctioning or failure of important hardware. Requires immediate attention and response of a technician to restore or maintain system stability. The urgency is less than in critical situations because of a lesser effect on service or system performance. For example, a minor alarm is generated if a secondary NSE-100 or NPE-G100 card fails or it is removed.

Minor alarm severity type Used for troubles that do not have a serious effect on service to customers or for alarms in hardware that are not essential to the operation of the system.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

MIB II MIB-II is the follow on to MIB-I which was the original standard SNMP MIB. MIB-II provided some much needed enhancements to MIB-I. MIB-II is very old, and most of it has been updated (that which has not is mostly obsolete). It includes objects that describe system related data, especially data related to a system's interfaces.

MPLS Multiprotocol Label Switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

MPLS interface An interface on which MPLS traffic is enabled. MPLS is the standardized version of Cisco original tag switching proposal. It uses a label forwarding paradigm (forward packets based on labels).

MTU Maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

N

NAS Network access server. Cisco platform or collection of platforms such as an AccessPath system which interfaces between the Internet and the circuit world (the PSTN).

NMS Network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

NHLFE Next Hop Label Forwarding Entry.

O

OID Object identifier. Values are defined in specific MIB modules. The Event MIB allows you or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, you or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and Boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

OIR Online Insertion and Removal.

OSM Optical Services Module

P

PA Port Adapter

PAP Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but identifies the remote end. The router or access server determines if that user is allowed access. PAP is supported only on PPP lines.

PEM Power Entry Module.

Polling Access method in which a primary network device inquires, in an orderly fashion, whether secondaries have data to transmit. The inquiry occurs in the form of a message to each secondary that gives the secondary the right to transmit.

POS Packet Over SONET

PPP Point-to-Point Protocol. Provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP is designed to work with several network layer protocols, such as IP, IPX, and ARA. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.

R

RADIUS Remote Authentication Dial-In User Service. RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

Read-only This variable can be used to monitor information only. For example, the locIPUnreach variable, whose access is read-only, indicates whether Internet Control Message Protocol (ICMP) packets concerning an unreachable address will be sent.

Read-write

This variable can be used to monitor information and to set a new value for the variable. For example, the tsMsgSend variable, whose access is read-write, determines what action to take after a message has been sent.

The possible integer values for this variable follow:

1 = nothing

2 = reload

3 = message done

4 = abort

RFC

Requests for Comments, started in 1969, form a series of notes about the Internet (originally the ARPANET). The notes discuss many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts, but also include meeting notes, opinions, and sometimes humor.

The RFC Editor is the publisher of RFCs and is responsible for the final editorial review of the documents. The RFC Editor also maintains a master file of RFCs, the RFC index, that you can search online here.

The specification documents of the Internet protocol suite, as defined by the Internet Engineering Task Force (IETF) and its steering group, the Internet Engineering Steering Group (IESG), are published as RFCs. Thus, the RFC publication process plays an important role in the Internet standards process. Go to the following URL for details:
http://www.cisco.com/en/US/docs/ios/11_0/mib/quick/reference/mtext.html

RMON

The Remote Network Monitoring MIB is a SNMP MIB for remote management of networks. RMON is one of the many SNMP based MIBs that are IETF Standards. RMON allows network operators to monitor the health of the network with a Network Management System (NMS). RMON watches several variables, such as Ethernet collisions, and triggers an event when a variable crosses a threshold in the specified time interval.

RSVP

Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP depends on IPv4. Also known as Resource Reservation Setup Protocol.

S

Scalar object

One type of managed object which is a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).

Security model

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.

SEEPROM

Serial Electrically Erasable Programmable Read-only Memory

SR Short Reach

SNMPv1 The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings. SNMPv1 uses 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.

SNMPv2 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.

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—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.

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.

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).

SONET Synchronous Optical Network. A physical layer interface standard for fiber optic transmission. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

SX Short wavelength

T

TE Traffic Engineered

Time stamp Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.

TLV Type Length Value. Dynamic format for storing data in any order. Used by Cisco's Generic ID PROM for storing asset information.

Traffic engineering tunnel A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

Trap An trap is an unsolicited (device initiated) message. The contents of the message might be simply informational, but it is mostly used to report real-time trap information. Since a trap is a UDP datagram, sole reliance upon them to inform you of network problems (i.e. passive network monitoring) is not wise. They can be used in conjunction with other SNMP mechanisms as in trap-directed polling or the SNMP inform mechanism can be used when a reliable fault reporting system is required.

Tunnel A secure communication path between two peers, such as routers.

U

UBR Unspecified bit rate. QOS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network, but there are no guarantees in terms of cell loss rate and delay. Compare with ABR (available bit rate), CBR, and VBR.

UDI Cisco Unique Device Identifier

UDP User Datagram Protocol.

V

VBR Variable bit rate. QOS class defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (RT) class and non-real time (NRT) class. VBR (RT) is used for connections in which there is a fixed timing relationship between samples. VBR (NRT) is used for connections in which there is no fixed timing relationship between samples, but that still need a guaranteed QOS.

VRF VPN Routing and Forwarding Tables.

VTP VLAN Trunking Protocol

W

WFQ Weighted Fair Queueing

Write-only This variable can be used to set a new value for the variable only. For example, the writeMem variable, whose access is write-only, writes the current (running) router configuration into nonvolatile memory where it can be stored and retained even if the router is reloaded. If the value is set to 0, the writeMem variable erases the configuration memory.

Write view A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that can be created or modified by users of the group.

X

XENPAK Fiber transceiver module which conforms to the 10GbE

Z

ZX Extended reach GBIC

INDEX

D

E

F

H

I

L

M

N

O

P

R

S

T

U

V