Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide

March 30, 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-15161-13

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco ASR 1000 Series Aggregation Services Routers MIB Specifications Guide

CONTENTS

APPENDIX B

INDEX

Preface

This guide describes the Cisco ASR 1000 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 1000 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 provides information about the status of the components.

This preface provides an overview of this guide, and contains the following sections:

- Revision History, page iii
- Audience, page xii
- Organization, page xiii
- Terminology and Definitions, page xiii
- Obtaining Documentation and Submitting a Service Request, page xiv

Revision History

The following Revision History tables record technical changes, additions, and corrections to this document. The tables show the release number and document revision number pertaining to the change, the date of the change, and a summary of the change.

Cisco IOS Release	Part Number	Publication Date
15.3(1)S	OL-15161-15	November 2012

Description of Changes

- Updated the Cisco ASR1000: 40G Native Ethernet Line Card support information for these MIBs:
  - ENTITY-MIB (RFC 4133)
  - ENTITY-SENSOR-MIB (RFC 3433)
  - ENTITY-STATE-MIB
  - CISCO-ENTITY-SENSOR-MIB
  - CISCO-ENTITY-ALARM-MIB

  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - IF-MIB (RFC 2863)
  - CISCO-IF-EXTENSION-MIB
  - ETHERLIKE-MIB (RFC 3635)
  - CISCO-ETHERLIKE-EXT-MIB
- Updated the SPA-8XT3/E3 support information for these MIBs:
  - ENTITY-MIB (RFC 4133)
  - ENTITY-SENSOR-MIB (RFC 3433)
  - ENTITY-STATE-MIB
  - CISCO-ENTITY-SENSOR-MIB
  - CISCO-ENTITY-ALARM-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - IF-MIB (RFC 2863)
  - CISCO-IF-EXTENSION-MIB
  - DS3-MIB (RFC 2496)

Cisco IOS Release	Part Number	Publication Date
15.2(4)S	OL-15161-14	July 2012

Description of Changes

- Added the following new MIBs:
  - CISCO-DYNAMIC-TEMPLATE-MIB
  - CISCO-SUBSCRIBER-SESSION-MIB
- Updated information about the ENTITY-MIB (RFC 4133)

Cisco IOS Release	Part Number	Publication Date
15.2(2)S	OL-15161-13	March, 2012

Description of Changes

- Added information about the CISCO-IMAGE-LICENSE-MGMT-MIB and CISCO-LICENSE-MGMT-MIB.
- Updated information about the CISCO-UNIFIED-FIREWALL-MIB.
- Updated information about the CISCO-IETF-PW-MIB and CISCO-IETF-PW-MPLS-MIB, indicating support for the SPA-2CHT3-CE-ATM SPA.

Cisco IOS Release	Part Number	Publication Date
15.1(00.15)S	OL-15161-12	December 26, 2011

Description of Changes

- Added information about the CISCO-RADIUS-EXT-MIB.
- Updated information about the CISCO-AAA-SERVER-MIB (removed the note indicating that the MIB is not supported on private AAA servers).

Cisco IOS Release	Part Number	Publication Date
15.2(1)S	OL-15161-11	November 28, 2011

Description of Changes

- Added new tables that contain information to support IPv6 addresses in addition to IPv4 addresses, in the CISCO-BGP4-MIB section.
- Added new notifications about support to IPv6 addresses in the CISCO-BGP4-MIB in the "Routing Protocol Notifications" section.

Cisco IOS Release	Part Number	Publication Date
15.1(3)S	OL-15161-10	July 22, 2011

Description of Changes

- Added support for these tables in the CISCO-CLASS-BASED-QOS-MIB:
  - cbQosMatchStmtCfgTable
  - cbQosMatchStmtStatsTable
  - cbQosSetStatsTable
- Added support for these MIBs on SPA-24CHT1-CE-ATM:
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-ENTITY-ALARM-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ENTITY-SENSOR-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - CISCO-IETF-PW-MIB
  - CISCO-IETF-PW-MPLS-MIB
  - CISCO-IF-EXTENSION-MIB
  - DS1-MIB (RFC 2495)
  - ENTITY-MIB (RFC 4133)
  - ENTITY-SENSOR-MIB (RFC 3433)

  - ENTITY-STATE-MIB
  - IF-MIB (RFC 2863)
- Added support for these MIBs on SPA-2CHT3-CE-ATM:
  - ATM-MIB
  - CISCO-AAL5-MIB
  - CISCO-ATM-EXT-MIB
  - CISCO-ATM-QOS-MIB
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-ENTITY-ALARM-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
  - CISCO-ENTITY-SENSOR-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB
  - CISCO-IETF-PW-ATM-MIB
  - CISCO-IETF-PW-MIB
  - CISCO-IETF-PW-MPLS-MIB
  - CISCO-IF-EXTENSION-MIB
  - DS3-MIB (RFC 2496)
  - ENTITY-MIB (RFC 4133)
  - ENTITY-SENSOR-MIB (RFC 3433)
  - ENTITY-STATE-MIB
  - IF-MIB (RFC 2863)

Cisco IOS Release	Part Number	Publication Date
15.1(2)S	OL-15161-09	March 29, 2011

Description of Changes

- Added the following new MIBs:
  - CISCO-ENTITY-PERFORMANCE-MIB
  - CISCO-SESS-BORDER-CTRLR-STATS-MIB
  - ETHER-WIS (RFC 3637)
  - CISCO-UBE-MIB
- Added a new alarm table, Table 3-40 “Alarms Supported for the Cisco ASR 1001 Series Routers FanTray Module”, for the FanTray module, in CISCO-ENTITY-ALARM-MIB.
- Added cevSpa1x10geWlV2 and cevSpa1pChoc3CemAtm to supported ceAlarmDescrVendorType in Table 3-27, “Alarms Supported for the Cisco ASR 1000 Series Routers SPAs”.
- Updated the following MIBs:
  - Added support information for the ASR1001 Router chassis in ENTITY-MIB (RFC 4133).

Cisco IOS Release	Part Number	Publication Date
15.1(1)S	OL-15161-08	November 2010

Description of Changes

- Added the following new MIBs:
  - CISCO-ETHERLIKE-EXT-MIB
  - CISCO-RTTMON-IP-EXT-MIB
  - ENTITY-STATE-MIB
  - CISCO-EVC-MIB
- Updated the following MIBs:
  - Added support information for the ASR1001 Router chassis in ENTITY-MIB (RFC 4133).
- Added a new alarm table, Table 3-40 "Alarms Supported for the Cisco ASR 1001 Series Routers FanTray Module", for the FanTray module, in CISCO-ENTITY-ALARM-MIB.
- Added information abut the new supported SPAs in CISCO-ENTITY-ALARM-MIB.
- Added new ceAlarmDescrVendorTypes to Table 3-27 "Alarms Supported for the Cisco ASR 1000 Series Routers SPAs".
- Added information about the support for the ASR1001 chassis on CISCO-ENTITY-VENDORTYPE-OID-MIB and CISCO-PRODUCTS-MIB.

Cisco IOS Release	Part Number	Publication Date
15.0(1)S	OL-15161-07	July 2010

Description of Changes

- Added the following new MIBs:
  - CISCO-ENTITY-QFP-MIB
  - HC-ALARM-MIB
  - CISCO-DIAL-CONTROL-MIB
  - CISCO-SIP-UA-MIB
  - CISCO-VOICE-COMMON-DIAL-CONTROL-MIB
  - CISCO-VOICE-DIAL-CONTROL-MIB
  - DIAL-CONTROL-MIB (RFC 2128)
- Updated the following MIBs:
  - CISCO-UNIFIED-FIREWALL-MIB
- Added new alarms to Table 3-36 "Alarms Supported for Cisco ASR 1000 Series Routers RP Module" and Table 3-39 "Alarms Supported for Cisco ASR 1000 Series Routers ESP/SIP Module"
- Added support for ASR 1013 chassis on CISCO-PRODUCTS-MIB.

Cisco IOS Release	Part Number	Publication Date
12.2(33)XNF	OL-15161-06	April 2010
12.2(33)XNF	OL-15161-06	February 2010

Description of Changes

- Added Table 3-63 listing support-matrix for cpmProcessTable and cpmProcessExtRevTable for ESP CPU.
- Updated Table 3-62 listing support-matrix for the CISCO-PROCESS-MIB cpmCPUTotalTable object.

Cisco IOS Release	Part Number	Publication Date
12.2(33)XNE	OL-15161-05	November 2009

Description of Changes

- Added the following new MIBs:
  - CISCO-NBAR-PROTOCOL-DISCOVERY-MIB
  - NHRP-MIB
- Updated the following MIBs for new constraints:
  - ATM-MIB
  - CISCO-ATM-EXT-MIB
  - CISCO-ATM-QOS-MIB
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-ENTITY-SENSOR-MIB
  - CISCO-IF-EXTENSION-MIB
  - ENTITY-MIB (RFC 4133)
  - NHRP-MIB
- Moved the following MIB from the Unsupported list to the Supported and Verified List
  - CISCO-MVPN-MIB
- Moved from the Supported and Unverified list to the Supported and Verified list:
  - CISCO-ATM-QOS-MIB
  - CISCO-IETF-FRR-MIB
  - CISCO-IPMROUTE-MIB
  - MPLS-TE-MIB
- Added new SPA to the CISCO-ENTITY-ALARM-MIB.
- Added SPA modules in Table 3-27, Alarms Supported for Cisco ASR 1000 Series Routers SPA module, under the CISCO-ENTITY-ALARM-MIB.
- Added Table 3-87, Table 3-88, for RP Module, SIP Module, SPA Module 0/0, and FP or ESP Module built-in with the CISCO ASR 1002-F chassis, under ENTITY-MIB (RFC 4133).

- Updated support matrix for the Table 3-62 CISCO-PROCESS-MIB.
- Added a note under ATM-MIB.
- Added the section Using ENTITY-ALARM-MIB to Monitor Entity Alarms in Appendix A under Managing Physical Entities.

Cisco IOS Release	Part Number	Publication Date
12.2(33)XND	OL-15161-04	June 2009

Description of Changes

- Added the following new MIBs:
  - CISCO-802-TAP-MIB
  - CISCO-IP-TAP-MIB
  - CISCO-LAG-MIB
  - CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB
  - CISCO-SESS-BORDER-CTRLR-EVENT-MIB
  - CISCO-TAP2-MIB
  - CISCO-TAP-MIB
  - CISCO-USER-CONNECTION-TAP-MIB
  - IEEE8023-LAG-MIB
  - RFC1213-MIB
- Updated the following MIBs for new constraints:
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-ENTITY-EXT-MIB
  - CISCO-IETF-PW-ATM-MIB
  - CISCO-IETF-PW-ENET-MIB
  - CISCO-IETF-PW-MIB
  - CISCO-IETF-PW-MPLS-MIB
- Updated versions for:
  - CISCO-CLASS-BASED-QOS-MIB
  - CISCO-ENTITY-EXT-MIB
- Added new SPAs to CISCO-ENTITY-ALARM-MIB.
- Added Table 3-25, Alarms Supported for Cisco ASR 1000 Series Routers WMA Virtual Ports under CISCO-ENTITY-ALARM-MIB.
- Updated Table 3-19, Alarms Supported for Cisco ASR 1000 Series Routers POS Ports, for vendorType information under CISCO-ENTITY-ALARM-MIB.
- Added SPA Modules to Table 3-27, Alarms Supported for Cisco ASR 1000 Series Routers SPA Module, under CISCO-ENTITY-ALARM-MIB.
- Added note for ASR1002-F Router support under CISCO-ENTITY-SENSOR-MIB and ENTITY-SENSOR-MIB (RFC 3433).

- Updated description for CISCO-ENTITY-VENDORTYPE-OID-MIB.
- Added Table 3-88, for RP Module, SIP Module, SPA Module 0/0, and FP or ESP Module built-in with the CISCO ASR 1002-F chassis, under ENTITY-MIB (RFC 4133).

Cisco IOS Release	Part Number	Publication Date
12.2(33)XNC	OL-15161-03	February 2009

Description of Changes

- Updated version CISCO-NETFLOW-MIB, CISCO-RTTMON-MIB, CISCO-VPDN-MGMT-MIB, and CISCO-IPMROUTE-MIB.
- Moved the following MIBs from Unsupported to Supported and Verified List
  - CISCO-IGMP-FILTER-MIB
- Moved the following MIBs from UnSupported to Supported and Unverified List:
  - CISCO-IETF-FRR-MIB
  - MPLS-TE-MIB
- Moved the following MIBs from Supported and Verified List to Unsupported List:
  - CISCO-SLB-EXT-MIB
  - CISCO-SLB-MIB
- Added the following MIBS to Supported and Verified MIBs list:
  - ATM-MIB
  - CISCO-AAL5-MIB
  - CISCO-ATM-EXT-MIB
  - CISCO-ATM-PVCTRAP-EXTN-MIB
  - CISCO-IETF-ATM2-PVCTRAP-MIB
  - CISCO-IETF-PW-MIB
  - CISCO-IETF-PW-ATM-MIB
  - CISCO-IETF-PW-MPLS-MIB
  - MPLS-L3VPN-STD-MIB (RFC 4382)
- Added the following MIBS to Supported and UnVerified MIBs list:
  - ATM-FORUM-ADDR-REG-MIB
  - ATM-FORUM-MIB
  - CISCO-ATM-QOS-MIB
- Added the following MIBS to Unsupported MIBs List:
  - ATM-ACCOUNTING-INFORMATION-MIB
  - ATM-SOFT-PVC-MIB
  - ATM-TRACE-MIB
  - CISCO-ATM2-MIB
  - CISCO-ATM-CONN-MIB

  - CISCO-ATM-RM-MIB
  - CISCO-ATM-TRAFFIC-MIB
  - CISCO-IETF-PW-ENET-MIB
  - CISCO-IETF-PW-FR-MIB
  - CISCO-IETF-PW-TDM-MIB
- Added SPA-1XOC3-ATM-V2 and SPA-3XOC3-ATM-V2 to SPA support list under CISCO-ENTITY-ALARM-MIB.
- Added the following tables to CISCO-ENTITY-ALARM-MIB:
  - Table 3-22 for T1/E1 ports
  - Table 3-23 for ATM
  - Table 3-37 for Unknown RP Module
- Update Table 3-36 for new RP Module Alarms.
- Added the following tables to ENTITY-MIB (RFC 4133):
  - Table 3-85 variation between entPhysicalTable values for harddisk in RP1 and RP2 modules
- Added a note indicating constraints due to 64-bit architecture in ASR1000 RP2 under CISCO-ENTITY-EXT-MIB, CISCO-PROCESS-MIB, and CISCO-ENHANCED-MEMPOOL-MIB
- Added notes under CISCO-FLASH-MIB and CISCO-ENTITY-ALARM-MIB.

Cisco IOS Release	Part Number	Publication Date
12.2(33)XNB	OL-15161-02	September 2008

Description of Changes

- Updated ASR 1002 Router behavioral changes under ENTITY-MIB (RFC 4133).
- Updated constraint information for CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-FLASH-MIB, CISCO-IETF-NAT-MIB, ENTITY-MIB (RFC 4133), and IP-MIB (RFC 4293).
- Added list of new SPAs supported under CISCO-ENTITY-ALARM-MIB.
- Added new alarm descriptions for the Cisco ASR 1000 Series Routers SPA modules in CISCO-ENTITY-ALARM-MIB.
- Added ciscoFlashFileType constraint for CISCO-FLASH-MIB.
- Added CISCO-IETF-NAT-MIB to manage Network Address Translation (NAT) operations on the Cisco ASR 1K router.
- Updated CISCO-PRODUCTS-MIB description to include CISCO ASR 1006, ASR 1004 and ASR 1002 OIDs support.
- Added dsx3LineStatusChange notification for DS3-MIB (RFC 2496).
- Moved CISCO-SLB-MIB and CISCO-SLB-EXT-MIB from Unsupported MIBs to Supported and Verified MIBs.
- Added ciscoSonetVTStatusChange constraint to CISCO-SONET-MIB.
- Added entPhysicalAssetAlias and entPhysicalAssetId constraints to ENTITY-MIB (RFC 4133).
- Added ifStackStatus constraint to IF-MIB (RFC 2863).
- Added SonetMediumTable and sonetSESthresholdSet constraints to SONET-MIB (RFC 2558).

- Added cefcModuleOperStatus and cefcModuleResetReason constraints to CISCO-ENTITY-FRU-CONTROL-MIB.
- Added cempMemPoolTable and cempMemBufferPoolTable constraints to CISCO-ENHANCED-MEMPOOL-MIB.
- Added ciscoFlashPartitionFileCount and ciscoFlashPhyEntIndex constraints to CISCO-FLASH-MIB.
- Added Table 3-19 to list alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers POS ports under CISCO-ENTITY-ALARM-MIB.
- Added Table 3-20 to list alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers CHOC3-STM1 ports under CISCO-ENTITY-ALARM-MIB.
- Added a note about no support for Aggregate Fragment Counters under CISCO-CLASS-BASED-QOS-MIB.
- Updated constraints for CISCO-FLASH-MIB.
- Added two new objects, cpmCPURisingThreshold and cpmCPUFallingThreshold, under constraints for CISCO-PROCESS-MIB.
- Updated constraints for CISCO-QINQ-VLAN-MIB.
- Added a new table,Table 3-82, that lists mapping between external label and entPhysicalParentRelPos values under ENTITY-MIB (RFC 4133).

Audience

This guide is intended for system and network administrators who must configure the Cisco ASR 1000 Series Router for operation and monitor its performance in the network.

This guide may also be useful for application developers who are developing management applications for the Cisco ASR 1000 Series Router.

Organization

This guide contains the following chapters:

Chapter	Description
Chapter 1, "Cisco ASR 1000 Series Aggregation Services Routers Overview,"	Provides background information about SNMP and its implementation on the Cisco ASR 1000 Series Router.
Chapter 2, "Configuring MIB Support,"	Provides instructions for configuring SNMP management support on the Cisco ASR 1000 Series Router.
Chapter 3, "Cisco ASR 1000 Series Routers MIB Specifications,"	Describes each MIB included on the Cisco ASR 1000 Series Router. In addition, constraints for each MIB are listed to indicated how a MIB is implemented on the router.
Chapter 4, "Monitoring Notifications,"	Describes the SNMP notifications, traps and informs, supported by the Cisco ASR 1000 Series Router. It provides 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 and Quality of Service (QoS).
Appendix B, "QoS MIB Implementation,"	Provides information about how to implement Quality of Service (QoS) in addition to a matrix that defines which objects support QoS policy actions.

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 (seethe Trap definition below). *Alarm* represents a condition which 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 1000 Series Aggregation Services Routers Overview

This chapter provides an overview of the enhanced management feature of the Cisco ASR 1000 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 1000 Series Routers 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. See the "SNMP Overview" section on page 1-3 for more information about SNMP and MIBs.

Using the Cisco ASR 1000 Series Routers enhanced management feature, you can:

- Manage and monitor Cisco ASR 1000 Series Routers resources through an SNMP-based network management system (NMS)
- Use SNMP **set** and **get** requests to access information in Cisco ASR 1000 Series Routers 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 on the Cisco ASR 1000 Series Routers. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. See Chapter 4, "Monitoring Notifications," for information about Cisco ASR 1000 Series Routers traps.

SNMP Versions

Cisco IOS software supports the following versions of SNMP:

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

SNMPv1 and SNMPv2c

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

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

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

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.internetsociety.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.

Related Information and Useful Links

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

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

TAC Information and FAQs

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

- Cisco TAC page for SNMP at: http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html. It provides links to general SNMP information and tips for using SNMP to gather data.
- Frequently Asked Questions (FAQs) about Cisco MIBs at: http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a0080094bc0.shtml.

SNMP Configuration Information

The following Cisco documents provide information about configuring SNMP:

- Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2, Part 3 System Management, "*Configuring SNMP Support*" at: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/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 1000 Series Routers. It includes the following sections:

- Determining MIB Support for Cisco IOS Releases, page 2-1
- Downloading and Compiling MIBs, page 2-1
- Enabling SNMP Support, page 2-3

Determining MIB Support for Cisco IOS Releases

Follow these steps to determine which MIBs are included in the Cisco IOS release running on the Cisco ASR 1000 Series Routers:

Step 1 Go to the Cisco MIBs Support page:

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

Step 2 Under Cisco Access Products, select **Cisco ASR1000** to display a list of MIBs supported on the Cisco ASR 1000 Series Routers.

Step 3 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 1000 Series Routers:

- Considerations for Working with MIBs, page 2-2
- Downloading MIBs, page 2-3
- Compiling MIBs, page 2-3

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

If you plan to integrate the Cisco ASR 1000 Series Routers with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile Cisco ASR 1000 Series Routers MIBs 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 1000 Series Routers 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 1000 Series Routers for SNMP support, follow these steps:

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 1000 Series Routers MIB Specifications

This chapter describes the Management Information Base (MIB) on the Cisco ASR 1000 Series Routers. It includes the following sections:

Cisco ASR 1000 Series Routers MIBs

Each MIB description lists relevant constraints about the MIB’s implementation on the Cisco ASR 1000 Series Routers platform. Any objects not listed in a 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 software release are fully supported by the Cisco ASR 1000 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 1000 Series Router platform.

For more information about the MIBs that are included in this releases, see the “Downloading and Compiling MIBs” section on page 2-1.

Cisco ASR 1000 Series Routers MIB Categories

The subsequent tables list the following categories of MIBs in the Cisco ASR 1000 Series Routers Image on the Cisco ASR 1000 Series Routers:

- Supported and verified MIBs (tested for Cisco ASR 1000 Series Routers)—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 1000 Series Routers)—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 1000 Series Routers)—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* in the following Cisco IOS release. The table lists the MIBs, corresponding notification name, and applicable MIB versions.

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image

MIB	Notification Name	Revision ID
ATM-MIB		9406072245Z
BGP4-MIB (RFC 1657)	bgpEstablished bgpBackwardTransition	9405050000Z
CISCO-AAA-SERVER-MIB	casServerStateChange	200001200000Z
CISCO-AAA-SESSION-MIB		200603210000Z
CISCO-AAL5-MIB		200309220000Z
CISCO-ATM-EXT-MIB		200301060000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

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-ATM-QOS-MIB	–	200206100000Z
CISCO-BGP4-MIB	cbgpFsmStateChange cbgpBackwardTransition cbgpPrefixThresholdExceeded cbgpPrefixThresholdClear cbgpPeer2EstablishedNotification cbgpPeer2BackwardTransNotification cbgpPeer2FsmStateChange cbgpPeer2BackwardTransition cbgpPeer2PrefixThresholdExceeded cbgpPeer2PrefixThresholdClear	200302240000Z
CISCO-BULK-FILE-MIB	cbfDefineFileCompletion	200108220000Z
CISCO-CBP-TARGET-MIB	–	200605240000Z
CISCO-CDP-MIB	–	200503210000Z
CISCO-CEF-MIB	cefResourceFailure cefPeerStateChange cefPeerFIBStateChange cefInconsistencyDetection	200601300000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-CLASS-BASED-QOS-MIB	–	200901260000Z
CISCO-CONFIG-COPY-MIB	ccCopyCompletion	200403170000Z
CISCO-CONFIG-MAN-MIB	ciscoConfigManEvent ccmCLIRunningConfigChanged ccmCTIDRolledOver	200608220000Z
CISCO-CONTEXT-MAPPING-MIB	–	200503170000Z
CISCO-DATA-COLLECTION-MIB	cdcVFileCollectionError cdcFileXferComplete	200210300530Z
CISCO-DIAL-CONTROL-MIB	–	200505260000Z
CISCO-DYNAMIC-TEMPLATE-MIB	–	200709060000Z
CISCO-EIGRP-MIB	–	200411160000Z
CISCO-EMBEDDED-EVENT-MGR-MIB	cEventMgrServerEvent cEventMgrPolicyEvent	200304160000Z
CISCO-ENHANCED-MEMPOOL-MIB	cempMemBufferNotify	200302240000Z[1]
CISCO-ENTITY-ALARM-MIB	ceAlarmAsserted ceAlarmCleared	9907062150Z
CISCO-ENTITY-EXT-MIB	–	200811240000Z
CISCO-ENTITY-FRU-CONTROL-MIB	cefcModuleStatusChange cefcPowerStatusChange cefcFRUInserted cefcFRURemoved cefcUnrecognizedFRU cefcFanTrayStatusChange	201112220000Z
CISCO-ENTITY-PERFORMANCE-MIB	–	201205150000Z
CISCO-ENTITY-QFP-MIB	–	201205150000Z
CISCO-ENTITY-SENSOR-MIB	entSensorThresholdNotification	200601010000Z
CISCO-ENTITY-VENDORTYPE-OID-MIB	–	200505050930Z
CISCO-ETHERLIKE-EXT-MIB	–	201006040000Z
CISCO-EVC-MIB	cevcEvcCreationNotification cevcEvcDeletionNotification cevcEvcStatusChangedNotification	200805010000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-FLASH-MIB	ciscoFlashCopyCompletionTrap ciscoFlashPartitioningCompletionTrap ciscoFlashMiscOpCompletionTrap ciscoFlashDeviceChangeTrap ciscoFlashDeviceInsertedNotif ciscoFlashDeviceRemovedNotif ciscoFlashDeviceInsertedNotifRev1 ciscoFlashDeviceRemovedNotifRev1	200403180000Z
CISCO-FRAME-RELAY-MIB	–	200010130000Z
CISCO-FTP-CLIENT-MIB	–	9710091700Z
CISCO-HSRP-EXT-MIB	–	9808030000Z
CISCO-HSRP-MIB	cHsrpStateChange	9808030000Z
CISCO-IETF-ATM2-PVCTRAP-MIB	atmIntfPvcFailuresTrap	9802030000Z
CISCO-IETF-BFD-MIB	ciscoBfdSessUp ciscoBfdSessDown	201104160000Z
CISCO-IETF-FRR-MIB	cmplsFrrProtected	200211051200Z
CISCO-IETF-ISIS-MIB	ciiDatabaseOverload ciiManualAddressDrops ciiCorruptedLSPDetected ciiAttemptToExceedMaxSequence ciiIDLenMismatch ciiMaxAreaAddressesMismatch ciiOwnLSPPurge ciiSequenceNumberSkip ciiAuthenticationTypeFailure ciiAuthenticationFailure ciiVersionSkew ciiAreaM	200508161200Z
CISCO-IETF-PPVPN-MPLS-VPN-MIB	cMplsNumVrfRouteMaxThreshCleared	200304171200Z
CISCO-IETF-PW-ATM-MIB	–	200504191200Z
CISCO-IETF-PW-ENET-MIB	–	200209221200Z
CISCO-IETF-PW-MIB	cpwVcDown cpwVcUp	200403171200Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-IETF-PW-MPLS-MIB	–	200302261200Z
CISCO-IF-EXTENSION-MIB	–	200311140000Z
CISCO-IGMP-FILTER-MIB	–	200111080000Z
CISCO-IMAGE-MIB	–	9508150000Z
CISCO-IMAGE-LICENSE-MGMT-MIB	cilmBootImageLevelChanged	200710160000Z
CISCO-IP-LOCAL-POOL-MIB	ciscoIpLocalPoolInUseAddrNoti	200304032000Z
CISCO-IPMROUTE-MIB	ciscoIpMRouteMissingHeartBeats	200503070000Z
CISCO-IPSEC-FLOW-MONITOR-MIB	cikeTunnelStart cikeTunnelStop cikeSysFailure cikeCertCrlFailure cikeProtocolFailure cikeNoSa cipSecTunnelStart cipSecTunnelStop cipSecSysFailure cipSecSetUpFailure cipSecEarlyTunTerm cipSecProtocolFailure cipSecNoSa	200010131800Z
CISCO-IPSEC-MIB	cipsIsakmpPolicyAdded cipsIsakmpPolicyDeleted cipsCryptomapAdded cipsCryptomapDeleted cipsCryptomapSetAttached cipsCryptomapSetDetached cipsTooManySAs	200008071139Z
CISCO-IPSEC-POLICY-MAP-MIB	–	200008171257Z
CISCO-IP-TAP-MIB	–	200403110000Z
CISCO-IP-URPF-MIB	cipUrpfIfDropRateNotify	200411120000Z
CISCO-LAG-MIB		

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-LICENSE-MGMT-MIB	clmgmtLicenseExpired clmgmtLicenseExpiryWarning clmgmtLicenseUsageCountExceeded clmgmtLicenseUsageCountAboutToExceed clmgmtLicenseInstalled clmgmtLicenseCleared clmgmtLicenseRevoked clmgmtLicenseEULAAccepted clmgmtLicenseNotEnforced clmgmtLicenseSubscriptionExpiryWarning clmgmtLicenseSubscriptionExtExpiryWarning clmgmtLicenseSubscriptionExpired clmgmtLicenseEvalRTUTransitionWarning clmgmtLicenseEvalRTUTransition	201104190000Z
CISCO-MVPN-MIB	ciscoMvpnMvrfChange	200402231200Z
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	–	200208160000Z
CISCO-NETFLOW-MIB	–	200604200000Z
CISCO-NTP-MIB	–	200307070000Z
CISCO-OSPF-MIB (draft-ietf-ospf-mib-update-05)	–	200307180000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
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-PING-MIB	ciscoPingCompletion	200108280000Z
CISCO-PPPOE-MIB	cPppoeSystemSessionThresholdTrap cPppoeVcSessionThresholdTrap	200102200000Z
CISCO-PROCESS-MIB	cpmCPURisingThreshold cpmCPUFallingThreshold	201005060000Z
CISCO-PRODUCTS-MIB	–	200505051930Z
CISCO-QINQ-VLAN-MIB	–	200411290000Z
CISCO-RADIUS-EXT-MIB		201005250000Z
CISCO-RF-MIB	ciscoRFSwactNotif ciscoRFProgressionNotif ciscoRFIssuStateNotifRev1	200803180000Z
CISCO-RTTMON-IP-EXT-MIB	–	200608020000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-RTTMON-MIB	rttMonConnectionChangeNotification rttMonTimeoutNotification rttMonThresholdNotification rttMonVerifyErrorNotification rttMonNotification rttMonLpdDiscoveryNotification rttMonLpdGrpStatusNotification	200701260000Z
CISCO-SIP-UA-MIB	–	200402190000Z
CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB	–	200808270000Z
CISCO-SESS-BORDER-CTRLR-EVENT-MIB	csbAlarmSubsystem csbAlarmSeverity csbAlarmID csbAlarmTime csbSBCServiceName csbDynamicBlackListSubFamily csbDynamicBlackListVpnId csbDynamicBlackListAddressType csbDynamicBlackListAddress csbDynamicBlackListTransportType csbDynamicBlackListPortNumber csbDynamicBlackListSrcBlocked csbAlarmDescription	200808270000Z
CISCO-SESS-BORDER-CTRLR-STATS-MIB	–	201009150000Z
CISCO-SONET-MIB	ciscoSonetSectionStatusChange ciscoSonetLineStatusChange ciscoSonetPathStatusChange	200205220000Z
CISCO-SUBSCRIBER-SESSION-MIB	csubJobFinishedNotify	200709060000Z
CISCO-SYSLOG-MIB	clogMessageGenerated	9508070000Z
CISCO-TAP2-MIB	ciscoTap2MIBActive ciscoTap2MediationTimedOut ciscoTap2MediationDebug ciscoTap2StreamDebug ciscoTap2Switchover	200611270000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-UBE-MIB	–	201011290000Z
CISCO-UNIFIED-FIREWALL-MIB	–	200509220000Z
CISCO-USER-CONNECTION-TAP-MIB	–	200708090000Z
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	–	9904010530Z
CISCO-VLAN-MEMBERSHIP-MIB	vmVmpsChange	200404070000Z
CISCO-VPDN-MGMT-MIB	cvpdnNotifSession cvpdnTrapDeadcacheEvent	200601200000Z
CISCO-VOICE-COMMON-DIAL-CONTROL-MIB	–	200903180000Z
CISCO-VOICE-DIAL-CONTROL-MIB	cvdcFallbackNotification	200905070000Z
CISCO-VOIP-TAP-MIB	–	200910010000Z
DIAL-CONTROL-MIB (RFC 2128)	dialCtlPeerCallInformation dialCtlPeerCallSetup	9609231544Z
DS1-MIB (RFC 2495)	dsx1LineStatusChange	9808011830Z
DS3-MIB (RFC 2496)	dsx3LineStatusChange	9808012130Z
ENTITY-MIB (RFC 4133)	entConfigChange	200508100000Z
ENTITY-SENSOR-MIB (RFC 3433)	–	200212160000Z
ENTITY-STATE-MIB	entStateOperEnabled entStateOperDisabled	200511220000Z
ETHER-WIS (RFC 3637)	–	200309190000Z
ETHERLIKE-MIB (RFC 3635)	–	200309190000Z
EVENT-MIB (RFC 2981)	mteTriggerFired mteTriggerRising mteTriggerFalling mteTriggerFailure mteEventSetFailure	200010160000Z
EXPRESSION-MIB	–	9802251700Z
FRAME-RELAY-DTE-MIB (RFC1315-MIB)	–	9511170836Z
IF-MIB (RFC 2863)	linkDown linkUp	9611031355Z
IGMP-STD-MIB (RFC 2933)	–	200009280000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
IP-FORWARD-MIB (RFC 4292)	–	200602010000Z
IP-MIB (RFC 4293)	–	200602020000Z
IPMROUTE-STD-MIB (RFC 2932)	–	200009220000Z
MPLS-L3VPN-STD-MIB (RFC 4382)	mplsL3VpnVrfUp mplsL3VpnVrfDown mplsL3VpnVrfRouteMidThreshExceeded mplsL3VpnVrfNumVrfRouteMaxThreshExceeded mplsL3VpnNumVrfSecIllglLblThrshExcd mplsL3VpnNumVrfRouteMaxThreshCleared	200601230000Z
MPLS-LDP-GENERIC-STD-MIB (RFC 3815)	–	200406030000Z
MPLS-LDP-STD-MIB (RFC 3815)	mplsLdpInitSessionThresholdExceeded mplsLdpPathVectorLimitMismatch mplsLdpSessionUp mplsLdpSessionDown	200406030000Z
MPLS-LSR-STD-MIB (RFC 3813)	mplsXCUp mplsXCDown	200406030000Z
MPLS-TE-MIB	mplsTunnelUp mplsTunnelDown mplsTunnelRerouted	200011211200Z
MPLS-VPN-MIB	mplsVrfIfUp mplsVrfIfDown mplsNumVrfRouteMidThreshExceeded mplsNumVrfRouteMaxThreshExceeded mplsNumVrfSecIllegalLabelThreshExceeded	200110151200Z
MSDP-MIB	msdpEstablished msdpBackwardTransition	9912160000Z
NHRP-MIB	–	9908260000Z
NOTIFICATION-LOG-MIB (RFC 3014)	–	200011270000Z
OLD-CISCO-SYS-MIB	–	
OSPF-MIB (RFC 1850)	–	9501201225Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
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
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
SNMPv2-MIB (RFC 1907)	coldStart warmStart linkDown linkUp authenticationFailure egpNeighborLoss	9511090000Z
SNMP-VIEW-BASED-ACM-MIB (RFC 2575)	–	9901200000Z
SONET-MIB (RFC 2558)	–	9810190000Z

Table 3-1 Supported and Verified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
TCP-MIB (RFC 4022)	–	200502180000Z
TUNNEL-MIB (RFC 4087)	–	200505160000Z
UDP-MIB (RFC 4113)	–	200505200000Z

1. For Release 02.03.02, the version for CISCO-ENHANCED-MEMPOOL-MIB is 200812050000Z.

Supported and Unverified MIBs

Table 3-2 lists the MIBs, notification name, and versions in the Cisco ASR 1000 Series Routers image that are *supported* and *unverified* in the following Cisco IOS release.

Table 3-2 Supported and Unverified Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image

MIB	Notification Name	Revision ID
ATM-FORUM-ADDR-REG-MIB	–	9606200322Z
ATM-FORUM-MIB	–	9606200322Z
HC-ALARM-MIB	–	200212160000Z
SNMP-USM-MIB (RFC 2574)	–	9901200000Z

Unsupported MIBs

Table 3-3 lists the MIBs, notification name, and versions in the Cisco ASR 1000 Series Routers image that are *unsupported* in the following Cisco IOS release.

Table 3-3 Unsupported Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image

MIB	Notification Name	Revision ID
ATM-ACCOUNTING-INFORMATION-MIB	–	9711050000Z
ATM-SOFT-PVC-MIB	atmSoftPvcCallFailuresTrap	9703010000Z
ATM-TRACE-MIB	–	UNKNOWN
CISCO-802-TAP-MIB	–	200607100000Z
CISCO-ATM2-MIB	–	9803040000Z
CISCO-ATM-CONN-MIB	–	200108060000Z
CISCO-ATM-RM-MIB	–	200101290000Z
CISCO-ATM-TRAFFIC-MIB	–	9705290000Z
CISCO-CALL-APPLICATION-MIB	–	9909220000Z
CISCO-ENHANCED-IMAGE-MIB	–	200501060000Z

Table 3-3 Unsupported Cisco ASR 1000 Series Routers MIBs in the Cisco ASR 1000 Series Routers Image (continued)

MIB	Notification Name	Revision ID
CISCO-ENTITY-ASSET-MIB	–	200207231600Z
CISCO-IETF-NAT-MIB	–	200103010000Z
CISCO-IETF-PW-FR-MIB	–	200312160000Z
CISCO-IETF-PW-TDM-MIB	–	200607210000Z
CISCO-LAG-MIB	–	200212130000Z
CISCO-SLB-EXT-MIB	cslbxFtStateChange	200302111000Z
CISCO-SLB-MIB	ciscoSlbVirtualStateChange ciscoSlbRealStateChange	200203180000Z
CISCO-TAP-MIB	cTapMIBActive, cTapMediationTimedOut cTapMediationDebug cTapStreamIpDebug	200401090000Z
CISCO-VOICE-ANALOG-IF-MIB	–	200510030000Z
CISCO-VOICE-IF-MIB	–	9803060000Z
IEEE8023-LAG-MIB	–	200006270000Z
OLD-CISCO-CHASSIS-MIB	–	UNKNOWN

ATM-ACCOUNTING-INFORMATION-MIB

The ATM-ACCOUNTING-INFORMATION-MIB contains objects to manage accounting information applicable to ATM connections.

Note This MIB is not verified in ASR 1000 Series Routers.

ATM-FORUM-ADDR-REG-MIB

The ATM-FORUM-ADDR-REG-MIB contains objects to manage information, such as ATM user-network interface (UNI) addresses and ports. This MIB also contains ATM address registration administration information.

Note This MIB is not supported in ASR 1000 Series Routers.

ATM-FORUM-MIB

The ATM-FORUM-MIB contains ATM object definitions and object identifiers (OIDs).

Note This MIB is not verified in ASR 1000 Series Routers.

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.

Note Effective from Cisco IOS Release 15.1(3)S, ATM-MIB is supported on SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-4 lists the constraints that the Cisco ASR1000 Series Router places on the objects in the ATM-MIB.

Table 3-4 ATM-MIB Constraints

MIB Object	Note
atmInterfaceDs3PlcpTable	Not used in Cisco ASR1000.
atmInterfaceTCTable	Not supported.
atmTrafficDescrParamTable	
• atmTrafficDescrType	Read only.
• atmTrafficDescrParam1	Read only.
• atmTrafficDescrParam2	Read only.
• atmTrafficDescrParam3	Read only.
• atmTrafficDescrParam4	Read only.
• atmTrafficDescrParam5	Read only.
• atmTrafficQoSClass	Read only.
atmVclTable	
• atmVclAdminStatus	Read only.
• atmVclReceiveTrafficDescrIndex	Read only.
• atmVclTransmitTrafficDescrIndex	Read only.
• atmVccAalType	Read only.
• atmVccAal5CpcsTransmitSduSize	Read only. Default value 4470.
• atmVccAal5CpcsReceiveSduSize	Read only. Default value 4470.
• atmVccAal5EncapsType	Read only.
• atmVclCrossConnectIdentifier	Read only.
• atmVclRowStatus	Read only.

Table 3-4 ATM-MIB Constraints (continued)

MIB Object	Note
• atmVclCastType • atmVclConnKind	Not supported. Not supported.
atmVcCrossConnectIndexNext	Not supported.
atmVcCrossConnectTable	Not implemented.
atmTrafficDescrParamIndexNext	Not supported.
atmVpCrossConnectTable	Not supported.
atmVpCrossConnectIndexNext	Not supported.
atmVplTable	Read only.

Note The ifType for the ifIndex object should be *atm(37)* type.

Note Shutting down "atm .0 subinterface" will only shut the atm main interface, and not the other atm subinterfaces.

Note The ATM mode is not supported on SPA-24CHT1-CE-ATM.

ATM-SOFT-PVC-MIB

The ATM-SOFT-PVC-MIB contains ATM Forum definitions of managed objects for ATM Soft Permanent Virtual Circuits. This MIB is not supported in this release.

BGP4-MIB (RFC 1657)

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

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

CISCO-802-TAP-MIB

The CISCO-802-TAP-MIB contains object to manage Cisco intercept feature for 802 streams (IEEE 802 intercept, layer 2) . This MIB is used along with CISCO-TAP2-MIB to intercept 802 traffic.

CISCO-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB contains objects to manage information such as authentication, authorization, and accounting (AAA) servers within the router and external to the router. This MIB provides:

- Configuration information for AAA servers, including identities of external AAA servers
- Statistics for AAA functions
- Status (state) information for AAA servers

MIB Constraints

The configuration objects in the MIB are read-only. To configure AAA servers, use the CLI commands **aaa new-model**, **aaa authentication ppp**, **aaa authorization**, **aaa accounting**, and **radius-server host**. Table 3-5 lists the constraints that the router places on the objects in the CISCO-AAA-SERVER-MIB.

Table 3-5 CISCO-AAA-SERVER-MIB Constraints

MIB Object	Notes
casConfigTable	
• casAddress	Read only.
• casAuthenPort	Read only. The default value is 1645.
• casAcctPort	Read only. The default value is1646.
• casKey	Read only. The value is shown as " " (null string) for security reasons.
• casConfigRowStatus	Read only.
casStatisTable	
• casAuthorTable • casAuthorRequest • casAuthorRequestTimeouts • casAuthorUnexpectedResponses • casAuthorServerErrorResponses • casAuthorIncorrectResponses • casAuthorResponseTime • casAuthorTransactionSuccesses • casAuthorTransactionFailures	For RADIUS servers, the value of these attributes is always 0. Only TACACS+ servers can have nonzero values. **Note** RADIUS servers do not make authorization requests.

CISCO-AAA-SESSION-MIB

The CISCO-AAA-SESSION-MIB contains information about accounting sessions based on authentication, authorization, and accounting (AAA) protocols.

CISCO-AAL5-MIB

The CISCO-AAL5-MIB contains objects to manage performance statistics for 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 from cAal5VccTable in RFC 1695.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-AAL5-MIB is supported on SPA-2CHT3-CE-ATM.

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.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-ATM-EXT-MIB is supported on SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-6 lists the constraint that the Cisco ASR 1000 Series Router places on the objects in the CISCO-ATM-EXT-MIB:

Table 3-6 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-PVCTRAP-EXTN-MIB

The CISCO-ATM-PVCTRAP-EXTN-MIB contains objects to extend the functionality for the ATM-MIB. This MIB provides additional notifications and traps for permanent virtual circuits (PVCs) on the CISCO ASR 1000. The CISCO-ATM-PVCTRAP-EXTN-MIB is supplemented by CISCO-IETF-ATM2-PVCTRAP-MIB.

CISCO-ATM-QOS-MIB

The CISCO-ATM-QOS-MIB contains objects to manage the following ATM QoS information:

- Traffic shaping on a per-VC basis
- Traffic shaping on a per-VP basis
- Per-VC queuing/buffering.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-ATM-QOS-MIB is supported on SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-7 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-ATM-QOS-MIB:

Table 3-7 CISCO-ATM-QOS-MIB Constraints

MIB Object	Notes
caqVccParamsTable	
• caqVccParamsCdv	Not supported.
• caqVccParamsCdvt	Not supported.
• caqVccParamsIcr	Not supported.
• caqVccParamsTbe	Not supported.
• caqVccParamsFrtt	Not supported.
• caqVccParamsNrm	Not supported.
• caqVccParamsInvTrm	Not supported.
• caqVccParamsInvCdf	Not supported.
• caqVccParamsAdtf	Not supported.
caqVpcParamsTable	
• caqVpcParamsAvailBw	Not supported.

CISCO-ATM2-MIB

The CISCO-ATM2-MIB contains objects to supplement ATM-MIB.

Note The CISCO-ATM2-MIB is not supported for any routers.

CISCO-ATM-CONN-MIB

The CISCO-ATM-CONN-MIB contains objects to extend the VPL/VCL table defined in RFC1695 for ATM switch connection management.

Note The CISCO-ATM-CONN-MIB is not supported for any routers.

CISCO-ATM-RM-MIB

The CISCO-ATM-RM-MIB contains object to provide resource management functionality. This MIB complements standard ATM MIBs for Cisco devices.

Note This CISCO-ATM-RM-MIB is not supported in this release.

CISCO-ATM-TRAFFIC-MIB

The CISCO-ATM-TRAFFIC-MIB contains objects that provide extension to traffic OIDs and variables defined in RFC1695.

Note The CISCO-ATM-TRAFFIC-MIB is not supported in this release.

CISCO-BGP4-MIB

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

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

Begining with Cisco IOS Release 15.2(1)S, CISCO-BGP4-MIB supports IPv6 addresses in addition to IPv4 addresses. To support IPv6-based peers, four new tables are added in the CISCO-BGP4-MIB:

- cbgpPeer2Table
- cbgpPeer2CapsTable

- cbgpPeer2AddrFamilyTable
- cbgpPeer2AddrFamilyPrefixTable

Note These four tables have flexible indexing to support both the IPv4 and IPv6 peers.

MIB Tables

Table 3-8 lists the tables in the CISCO-BGP4-MIB.

Table 3-8 CISCO-BGP4-MIB Tables

MIB Table	Description
cbgpRouteTable	Contains information about the routes to the destination networks from all the BGP4 peers.
cbgpPeerTable	Contains information about the connections with the BGP peers, one entry for each BGP peer.
cbgpPeerCapsTable	Contains information about the capabilities supported by a peer. The capabilities of a peer are received while establishing the BGP connection.
cbgpPeerAddrFamilyTable	Contains information related to the address families supported by a peer.
cbgpPeerAddrFamilyPrefixTable	Contains prefix-related information for the address families supported by a peer.
cbgpPeer2Table	Contains information about the connection with the BGP peers, one entry for each BGP peer. This table supports IPv4 and IPv6 peers.
cbgpPeer2CapsTable	Contains information about the capabilities supported by a BGP peer. The capabilities of a peer are received while establishing the BGP connection. This table supports IPv4 and IPv6 peers.
cbgpPeer2AddrFamilyTable	Contains information related to the address families supported by a BGP peer. This table supports IPv4 and IPv6 peers.
cbgpPeer2AddrFamilyPrefixTable	Contains prefix-related information for the address families supported by a peer. This table supports IPv4 and IPv6 peers.

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 3-9 lists the constraints that the router places on the objects in the CISCO-BULK-FILE-MIB.

Table 3-9 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-CALL-APPLICATION-MIB

The CISCO-CALL-APPLICATION-MIB manages the call applications on a network device. A call application is a software module that processes data, voice, video, and fax calls.

Note This MIB is not supported in the ASR 1000 Series Routers.

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. These features can be enabled in a feature-specific manner or through the Class-based Policy Language (CPL).

The CISCO-CBP-TARGET-MIB abstracts the knowledge of the specific types of targets from the class-based policy feature-specific MIB definitions.

MIB Constraints

The configuration objects in the MIB are read-only. To configure AAA servers, use the CLI commands **aaa new-model**, **aaa authentication ppp**, **aaa authorization**, **aaa accounting**, and **radius-server host**. Table 3-10 lists the constraints that the router places on the objects in the CISCO-CBP-TARGET-MIB.

Table 3-10 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 3-11 lists the constraints that the router places on the objects in the CISCO-CDP-MIB.

Table 3-11 CISCO-CDP-MIB Constraints

MIB Object	Notes
cdpCtAddressTable	Not supported.
cdpGlobalLastChange	Not supported.
cdpGlobalDeviceIdFormatCpb	Not supported.

Table 3-11 CISCO-CDP-MIB Constraints (continued)

MIB Object	Notes
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 3-12 lists the constraints that the router places on the objects in the CISCO-CEF-MIB.

Table 3-12 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 (CEF) is a high-speed switching mechanism that a router uses to forward packets from the inbound to the outbound interface.

CISCO-CLASS-BASED-QOS-MIB

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

To understand how to navigate the CISCO-CLASS-BASED-QOS-MIB tables, it is important to understand the relationship among different QoS objects. QoS objects consists of:

- Match Statement—The specific match criteria to identify packets for classification purposes.
- Class Map—A user-defined traffic class that contains one or more match statements used to classify packets into different categories.
- Feature Action—AQoS feature. Features include police, traffic shaping, queueing, random detect, and packet marking. After the traffic has been classified, apply actions to each traffic class.
- Policy Map—Auser-defined policy that associates a QoS feature action to the user-defined class map.

- Service Policy—Apolicy map that has been attached to an interface.

The MIB uses the following indices 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—includes all class maps, policy maps, match statements, and feature action configuration parameters. Might have multiple identical instances. Multiple instances of the same QoS feature share a single configuration object, which is identified by cbQosConfigIndex.
- Runtime Statistics instances—Includes summary counts and rates 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 The Policing, Shaping, Queuing, and WRED features are not supported for the SPA-1CHOC3-CE-ATM.

Note The SNMP does not support the *bandwidth remaining ratio* configuration. Bandwith is displayed in *kbps*.

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.

Note Only the MPLS EXP Bit Setting Marking feature is supported for the SPA-1CHOC3-CE-ATM.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-CLASS-BASED-QOS-MIB is supported on SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-13 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-CLASS-BASED-QOS-MIB.

Table 3-13 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.
cbQosQueueingMaxQDepth	Not supported.

Table 3-13 CISCO-CLASS-BASED-QOS-MIB Constraints

MIB Object	Notes
cbQosREDECNMarkPktOverflow	Not supported.
cbQosREDECNMarkPkt	Not supported.
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.

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
- The running configuration to the startup configuration and startup to running
- The startup or running configuration files to and from a local Cisco IOS 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 3-14 lists the constraints that the Cisco ASR 1000 Series Routers place 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 3-14 CISCO-DATA-COLLECTION-MIB Constraints

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

CISCO-DIAL-CONTROL-MIB

The CISCO-DIAL-CONTROL-MIB module is an extension of RFC 2128, and defines the callHistoryTable that stores information pertaining to earlier calls.

CISCO-DYNAMIC-TEMPLATE-MIB

The CISCO-DYNAMIC-TEMPLATE-MIB contains objects that describe the dynamic templates. A dynamic template is a set of configuration attributes that a system can dynamically apply to a target.

MIB Tables

Table 3-15 lists the tables in the CISCO-DYNAMIC-TEMPLATE-MIB.

Table 3-15 CISCO-DYNAMIC-TEMPLATE-MIB Tables

MIB Table	Description
cdtTemplateTable	Lists the dynamic templates maintained by the system, including those that are locally configured on the system, and those that are pushed to the system by external policy servers.
cdtTemplateTargetTable	Lists the targets associated with one or more dynamic templates.
cdtTemplateAssociationTable	Lists the templates associated with each target.
cdtTemplateUsageTable	Contains a list of targets that use each dynamic template.
cdtTemplateCommonTable	Contains attributes that relate to all the dynamic templates.
cdtIfTemplateTable	Contains attributes that relate to the interface configuration.
cdtPppTemplateTable	Contains attributes that relate to PPP connection configuration.
cdtPppPeerIpAddrPoolTable	Contains a prioritized list of named pools for each PPP template.
cdtEthernetTemplateTable	Contains attributes pertaining to the dynamic interfaces initiated on ethernet virtual interfaces or automatically created VLANs.
cdtSrvTemplateTable	Contains attributes pertaining to a service.

MIB Constraints

Table 3-16 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-DYNAMIC-TEMPLATE-MIB. Any MIB object not listed in this table is implemented as defined in the MIB.

Table 3-16 CISCO-DYNAMIC-TEMPLATE-MIB Constraints

MIB Object	Notes
cdtTemplateTable	
• cdtTemplateName	Read only.
• cdtTemplateUsageCount	Read only.
• cdtTemplateStatus	Read only.
• cdtTemplateStorage	Not implemented.
• cdtTemplateType	Not implemented.
• cdtTemplateSrc	Not implemented.
cdtTemplateAssociationTable	
• cdtTemplateAssociationName	Read only.
cdtTemplateUsageTable	
• cdtTemplateUsageTargetType	Read only.
• cdtTemplateUsageTargetId	Read only.
cdtTemplateTargetTable	Not implemented.

Table 3-16 CISCO-DYNAMIC-TEMPLATE-MIB Constraints (continued)

MIB Object	Notes
cdtTemplateCommonTable	Not implemented.
cdtIfTemplateTable	Not implemented.
cdtPppTemplateTable	Not implemented.
cdtPppPeerIpAddrPoolTable	Not implemented.
cdtEthernetTemplateTable	Not implemented.
cdtSrvTemplateTable	Not implemented.

CISCO-EIGRP-MIB

The CISCO-EIGRP-MIB contains objects to manage Enhanced Interior Gateway Protocol (EIGRP). EIGRP is a Cisco proprietary distance vector routing protocol, based on the Diffusing Update Algorithm (DUAL). DUAL defines the method to identify loop-free paths through a network.

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-IMAGE-MIB

The CISCO-ENHANCED-IMAGE-MIB provides information about events running on the system. The MIB modular operating systems.

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.

Note The Cisco ASR1000 RP2 supports 64-bit architecture. Effective from Cisco IOS Release 15.2(4)S onwards, the CISCO-PROCESS-MIB supports 64-bit architecture.

MIB Constraints

The CISCO-ENHANCED-MEMPOOL-MIB is supported only in the Active RP module. Table 3-17 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-ENHANCED-MEMPOOL-MIB.

Table 3-17 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.
• 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 1000 Series Routers 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:

- SPA-10X1GE-V2
- SPA-1X10GE-L-V2
- SPA-1XCHSTM1/OC3
- SPA-1XCHOC12/DS0
- SPA-1XOC12-POS
- SPA-1XOC3-ATM-V2
- SPA-1XOC48POS/RPR: 1 -port OC48/STM16 POS/RPR SFP Optics SPA
- SPA-2X1GE-V2
- SPA-2XCT3/DS0 with T1 channels (Serial interface)
- SPA-2XCT3/DS0 without the T1 channels
- SPA-2XOC12-POS: 2-port OC12 POS SPA
- SPA-2XOC3-POS
- SPA-2XOC48POS/RPR
- SPA-2XT3/E3 as Serial interface only (not as controller).
- SPA-3XOC3-ATM-V2
- SPA-4XOC12-POS: 4-port OC12 POS SPA
- SPA-4XOC48POS/RPR
- SPA-4XT-Serial
- SPA-4XT-Serial as Serial interface only
- SPA-5X1GE-V2
- SPA-8X1FE-TX-V2
- SPA-8X1GE-V2
- SPA-8XCHT1/E1
- SPA-8XOC12-POS: 8-port OC12 POS SPA
- SPA-8XOC3-POS: 8-port OC3 POS SPA
- SPA-DSP
- SPA-2X1GE-SYNCE
- SPA-1X10GE-WL-V2
- SPA-1CHOC3-CE-ATM
- ASR1001-IDC-4XT3
- ASR1001-IDC-2XOC3POS
- ASR1001-IDC-HDD
- ASR1001-IDC-4XGE
- ASR1001-IDC-8XT1E1
- SPA-OC192POS-XFP: 1-port OC192/STM64 POS/RPR XFP Optics SPA
- SPA-WMA-K9 : Butler (WebEx) SPA: 1-port WebEx SPA
- SPA-1XOC12-ATM-V2 : 1-port OC12/STM4 ATM Shared Port Adapter

All the other interface types are not supported for this release. Sensor Alarms are not supported for SPA sensors and transceiver sensors in this release.

For more information on this MIB, refer Appendix A, "CISCO-ENTITY-ALARM-MIB."

Note The CISCO-ENTITY-ALARM-MIB is supported on the ASR 1001 chassis.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-ENTITY-ALARM-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note The alarms supported for the POS Ports of the Cisco ASR 1000 Series Routers are also supported for SPA-1X10GE-WL-V2 for the Ethernet WIS port.

Note Effective from Cisco IOS Release 15.3(1)S, CISCO-ENTITY-ALARM-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

MIB Constraints

Table 3-18 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-ENTITY-ALARM-MIB.

Table 3-18 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 1000 Series Routers 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) that uniquely identifies an event relative to a physical entity in the Cisco ASR 1000 Series Routers.

Table 3-19 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Router POS ports.

Table 3-19 Alarms Supported for Cisco ASR 1000 Series Routers POS Ports

Physical Entity	entPhysicalVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Interface	cevPortPOS cevPortOc3 cevPortOc12 cevPortOc48 cevPortOc192	critical	Section Loss of Signal Failure.
		critical	Section Loss of Frame Failure.
		critical	Section Out of Frame Alignment.
		critical	Section J0 mismatch.
		critical	Section Bit Interleaved Parity.
		critical	Line Alarm Indication Signal.
		critical	Line Remote Failure Indication.
		critical	Line Bit Interleaved Parity.
		critical	Line Far End Block Errors.
		critical	Path Alarm Indication Signal.
		critical	Path Remote Failure Indication.
		critical	Path Loss of Pointer.
		critical	Path Bit Interleaved Parity.
		critical	Path Far End Block Errors.
		critical	Protection Switch Byte Failure.
		critical	Path Pointer justifications.
		critical	Path positive pointer stuff event.
		critical	Path negative pointer stuff event.
		critical	Path Payload Label Mismatch.
		critical	Path payload Unequipped.
		critical	Count of APS.
		critical	Receiver Data out of Lock Failure.
		critical	Signal Failure Alarm.
		critical	Signal Degrade Alarm.
		critical	Threshold Cross Alarm - B1.
		critical	Threshold Cross Alarm - B2.
		critical	Threshold Cross Alarm - B3.
		critical	Port Link Down Alarm.
		critical	Path Trace Identifier Mismatch.
		critical	Path Trace Identifier Unstable.
		minor	Signal Failure Alarm/B3 errors.
		minor	Loss of Multiframe.
		critical	Loss of Multiframe.
		info	Port Administrative Down Alarm.

Table 3-20 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Router CHOC3-STM1 and CHOC12 ports.

Table 3-20 Alarms Supported for Cisco ASR 1000 Series Routers CHOC3-STM1 & CHOC12 Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Channelized SONET interface	cevPortChOc3Stm1/cevPortChOcX	critical	Section Loss of Frame Failure.
	cevPortChOc3Stm1/cevPortChOcX	critical	Section Out of Frame Alignment.
	cevPortChOc3Stm1/cevPortChOcX	critical	JOMM
	cevPortChOc3Stm1/cevPortChOcX	critical	Section Bit Interleaved Parity.
	cevPortChOc3Stm1/cevPortChOcX	critical	Line Alarm Indication Signal.
	cevPortChOc3Stm1/cevPortChOcX	critical	Line Remote Defect Indication.
	cevPortChOc3Stm1/cevPortChOcX	critical	Line Bit Interleaved Parity.
	cevPortChOc3Stm1/cevPortChOcX	critical	Line Far End Block Errors.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Alarm Indication Signal.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Remote Defect Indication.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Loss of Pointer.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Bit Interleaved Parity.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Far End Block Errors.
	cevPortChOc3Stm1/cevPortChOcX	critical	Protection Switch Byte Failure.
	cevPortChOc3Stm1/cevPortChOcX	info	PNEWPTR
	cevPortChOc3Stm1/cevPortChOcX	critical	Path positive pointer stuff event.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path negative pointer stuff event.
	cevPortChOc3Stm1/cevPortChOcX	critical	Path Payload Label Mismatch.
	cevPortChOc3Stm1/cevPortChOcX	critical	PUNEQ

Table 3-20 Alarms Supported for Cisco ASR 1000 Series Routers CHOC3-STM1 & CHOC12 Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
	cevPortChOc3Stm1/cevPortChOcX	critical	PTIM
	cevPortChOc3Stm1/cevPortChOcX	critical	PTIU
	cevPortChOc3Stm1/cevPortChOcX	critical	Count of APS.
	cevPortChOc3Stm1/cevPortChOcX	critical	Receiver Data out of Lock Failure.
	cevPortChOc3Stm1/cevPortChOcX	critical	Signal Failure Alarm.
	cevPortChOc3Stm1/cevPortChOcX	critical	Signal Degrade Alarm.
	cevPortChOc3Stm1/cevPortChOcX	critical	Signal Failure Alarm – B3.
	cevPortChOc3Stm1/cevPortChOcX	critical	Signal Degrade Alarm – B3.
	cevPortChOc3Stm1/cevPortChOcX	critical	Threshold Cross Alarm - B1.
	cevPortChOc3Stm1/cevPortChOcX	critical	Threshold Cross Alarm - B2.
	cevPortChOc3Stm1/cevPortChOcX	critical	Threshold Cross Alarm - B3.
	cevPortChOc3Stm1/cevPortChOcX	critical	LOM
	cevPortChOc3Stm1/cevPortChOcX	critical	FEPLF
	cevPortChOc3Stm1/cevPortChOcX	critical	MODEMM
	cevPortChOc3Stm1/cevPortChOcX	critical	CHANNELMM

Table 3-21 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers T3/E3 ports. The entries for T3/E3 ports mentioned in this table are always populated for ceAlarmDescrTable and ceAlarmDescrVendorType, irrespective of the presence or absence of the ports.

Table 3-21 Alarms Supported for Cisco ASR 1000 Series Routers T3/E3 Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
T3/E3 port	cevPortCT3 cevPortT3E3	major	Transmitter is sending remote alarm.
		major	Transmitter is sending AIS.

Table 3-21 Alarms Supported for Cisco ASR 1000 Series Routers T3/E3 Ports (continued)

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
		major	Receiver has loss of signal.
		major	Receiver is receiving AIS.
		major	Receiver has loss of frame.
		major	Receiver has remote alarm.
		major	Receiver has idle signal.
		major	Other failure.
		major	DS3 port link down.
		info	DS3 port admin down.

Table 3-22 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers T1/E1 ports. 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 3-22 Alarms Supported for Cisco ASR 1000 Series Routers T1/E1 Ports

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

Table 3-23 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers ATM ports

Table 3-23 Alarms Supported for the Cisco ASR 1000 Series Routers ATM Ports

Physical Entity	entPhysicalVendorType	ceAlarmDescrSeverity	ceAlarmDescrText
ATM interface	cevPortAtm	critical	Section Loss of Signal Failure
		critical	Section Loss of Frame Failure
		critical	Section Out of Frame Alignment
		critical	Section Bit Interleaved Parity
		critical	Line Alarm Indication Signal
		critical	Line Remote Failure Indication
		critical	Line Bit Interleaved Parity
		critical	Line Far End Block Errors
		critical	Path Alarm Indication Signal
		critical	Path Remote Failure Indication
		critical	Path Loss of Pointer
		critical	Path Bit Interleaved Parity
		critical	Path Far End Block Errors
		critical	Protection Switch Byte Failure
		critical	Path Pointer justifications
		critical	Path positive pointer stuff event
		critical	Path negative pointer stuff event
		critical	Path Payload Label Mismatch
		critical	Path payload Unequipped
		critical	Count of APS
		critical	Receiver Data out of Lock Failure
		critical	Signal Failure Alarm
		critical	Signal Degrade Alarm
		critical	Signal Failure B3 Alarm
		critical	Signal Degrade B3 Alarm
		critical	Threshold Cross Alarm - B1
		critical	Threshold Cross Alarm - B2
		critical	Threshold Cross Alarm - B3
		critical	Loss of Multiframe
		critical	Loss of Cell Delineation
		critical	Physical Port Link Down Alarm
ATM interface	cevPortAtm	info	Physical Port Administrative State Down Alarm

Table 3-24 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers over Gigabit Ethernet (GE) ports.

Table 3-24 Alarms Supported for the Cisco ASR 1000 Series Routers GE Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
GE port	cevPortGE	critical	Physical port link down.
		info	Physical port administrative state down.
		info	Physical port not configured.

Table 3-25 lists the alarm descriptions and severity levels for the WMA Virtual ports in the Cisco ASR 1000 Series Routers.

Table 3-25 Alarms Supported for the Cisco ASR 1000 Series Routers WMA Virtual Ports

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescrSeverity	ceAlarmDescrText
Service Engine interface	cevPortSEInternal	critical	Physical Port Link Down
		info	Physical Port Administrative State Down

Table 3-26 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers SFP Container.

Table 3-26 Alarms Supported for Cisco ASR 1000 Series Routers SFP Container

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText	Scenario
SFP container	cevContainerSFP	critical	Transceiver missing	When the interface is *not* using RJ-45 and is in link down state.
SFP container	cevContainerSFP	info	Transceiver missing	When the interface is configured to use RJ-45 (only applicable to SPA-2X1GE) or is in admin down state.

Table 3-27 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers SPAs.

Table 3-27 Alarms Supported for the Cisco ASR 1000 Series Routers SPAs

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
SPA	cevSpa10pGeV2 cevSpa10pGeV2 cevSpa1p10GeXfpV2 cevSpa1p10GeXfpV2 cevSpa1pChOc3Stm1 cevSpa1pOc12Pos cevSpa1pOc192PosRprXfp cevSpa1pOc48PosSfp cevSpa2pCT3 cevSpa2pCT3 cevSpa2pGeV2 cevSpa2pGeV2 cevSpa2pOc12Pos cevSpa2pOc3Atm cevSpa2pOc3Pos cevSpa2pOc48PosRprHH cevSpa2pT3E3Serial cevSpa24pCt1e1CemAtm cevSpa2pCt3e3CemAtm cevSpa4pOc48PosSfp cevSpa4xoc12Pos cevSpa4xtSerial cevSpa5pGeV2 cevSpa5pGeV2 cevSpa8pCT1E1 cevSpa8pCT1E1 cevSpa8pGeV2 cevSpa8pOc12Pos cevSpa8xfeTxV2 cevSpa8xoc3Pos cevSpaWmaSw cevSpa1pOc12Atm cevSpa1pChoc12Ds0 cevSpaDsp cevSpa2pGeSynce cevSpa1x10geWlV2 cevSpa1pChoc3CemAtm	major	Unknown state
		major	Boot state
		major	Disabled
		critical	Failed
		major	Stopped

Table 3-28 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers sensors.

Table 3-28 Alarms Supported for Cisco ASR 1000 Series Routers 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	Readingbelow normal (Shutdown).
		critical	Reading below normal.
		major	Reading below normal.
		minor	Reading below normal.

Note These alarms are not supported for SPA and XCVR sensors. You can use CISCO-ENTITY-SENSOR-MIB to monitor the alarms listed in the Table 3-28.

Table 3-29 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers SPA containers.

Table 3-29 Alarms Supported for Cisco ASR 1000 Series Routers SPA Container

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

Table 3-30 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers USB ports.

Table 3-30 Alarms Supported for Cisco ASR 1000 Series Routers USB Ports

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

Table 3-31 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers RP containers.

Table 3-31 Alarms Supported for Cisco ASR 1000 Series Routers RP Container

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RP container	cevContainerASR1000RP Slot	critical	RP removed OIR alarm
		critical	RP stopped responding

Table 3-32 lists the alarm descriptions and severity levels for the Cisco ASR 1001 Series Routers h hard disk containers.

Table 3-32 Alarms Supported for the Cisco ASR 1001 Series Router Hard Disk Container

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescrSeverity	ceAlarmDescrText
hard disk container	cevContainerHardDiskSlot	major	Hard disk missing.

Table 3-33 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers FP containers.

Table 3-33 Alarms Supported for Cisco ASR 1000 Series Router FP Container

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
FP container	cevContainerASR1000FP Slot	critical	FP removed OIR alarm
		critical	FP stopped responding

Note The Forwarding Processor (FP) does not register to OIR alarm because it is not a FRU entity in the CISCO-ENTITY-ALARM-MIB for ASR1002-F chassis.

Table 3-34 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers SIP containers.

Table 3-34 Alarms Supported for Cisco ASR 1000 Series Routers SIP Container

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
SIP container	cevContainerASR1000CC Slot	critical	CC removed OIR alarm.
		critical	CC stopped responding.

Table 3-35 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers power supply bay.

Table 3-35 Alarms Supported for Cisco ASR 1000 Series Routers Power Supply Bay

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Power Supply Bay	cevContainerASR1000PowerSupplyBay	critical	Power supply/Fan module missing.

Table 3-36 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers RPs.

Table 3-36 Alarms Supported for Cisco ASR 1000 Series Routers RP Module

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RP Module	cevModuleASR1000RP1 cevModuleASR1000RP2 cevModuleASR1002RP1	major	Unknown state.
		major	Boot state.
		major	Disabled.
		critical	Incompatible
		critical	CPLD incompatible
		critical	Active RP CPLD incompatible
		critical	Failed.
		critical	Cutover.
		major	Secondary failure.
		major	Secondary removed.
		major	Secondary not synchronized.
		critical	No working ESP.
		major	Harddisk Missing[1].

[1] Not applicable for cevModuleASR1002RP1.

Note The Cisco ASR 1002 Router does not have harddisk, so the 'Harddisk Missing' alarm is not registered for cevModuleASR1002RP1.

The vendor OID for the RP Module is set to cevModuleASR1000UnknownRP for the following conditions:

- The secondary RP is loaded with the valid image and the RP Module is not operational.
- The software does not understand the hardware subtype of the secondary RP Module.
- The secondary RP is loaded with an invalid image.

Prior to RLS3 release, cevModuleASR1000UnknownRP alarm was registered for all the RP alarms, this behavior is changed from Release 3 and only the Module alarms are registered.

Table 3-37 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers Unknown RP Module.

Table 3-37 Alarms Supported for Cisco ASR 1000 Series Routers Unknown RP Modules

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
RP Module	cevModuleASR1000UnknownRP	major	Unknown state.
		major	Boot state.
		major	Disabled.
		critical	Failed.
		critical	Stopped.

Table 3-38 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers Power Supply Module.

Table 3-38 Alarms Supported for Cisco ASR 1000 Series Routers Power Supply Module

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
Power Supply Modules	cevPowerSupplyASR1006AC	critical	Power Supply Failure.
		critical	All Fans Failed.
		critical	Multiple Fan Failures.
		major	Fan 0 Failure.
		major	Fan 1 Failure.
		major	Fan 2 Failure.

Note ASR1002 and ASR1002-F have two fans each.

Table 3-39 lists the alarm descriptions and severity levels for the Cisco ASR 1000 Series Routers ESP modules.

Table 3-39 Alarms Supported for Cisco ASR 1000 Series Routers ESP/SIP Module

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
ESP Module	cevModuleASR1000ESP10	major	Unknown state.
	cevModuleASR1000SIP10	major	Boot State.
	cevModuleASR1000ESP5	major	Disabled.
	cevModuleASR1000ESP20	critical	Incompatible
	cevModuleASR1002SIP10	critical	CPLD incompatible
	cevModuleASR1000SIP40	critical	Active RP CPLD incompatible
	cevModuleASR1000ESP10N	critical	Failed.
		major	Stopped.

Table 3-40 lists the alarms that the FanTray module of the Cisco ASR 1001 Router support.

Table 3-40 Alarms Supported for the Cisco ASR 1001 Series Routers FanTray Module

Physical Entity	ceAlarmDescrVendorType	ceAlarmDescr Severity	ceAlarmDescrText
FanTray Modules	cevFanASR1001FanTray	critical	FanTray/Module Failure.
		critical	All Fans Failed.
		critical	Multiple Fan Failures.
		major	Fan 0 failure.
		major	Fan 1 failure.
		major	Fan 2 failure.
		major	Fan 3 failure.
		major	Fan 4 failure.
		major	Fan 5 failure.
		major	Fan 6 failure.

Note FanTray is supported on the ASR1001 Router chassis having seven fans and no sensors.

Note The ceAlarmHistTable contains alarm data asserted/cleared in the current active RP. It does not retain the alarms asserted/cleared in the previous active RP. The data contained in ceAlarmHistTable is refreshed after a switchover.

CISCO-ENTITY-ASSET-MIB

The CISCO-ENTITY-ASSET-MIB provides asset tracking information (ceAssetTable) for the physical components in the ENTITY-MIB (RFC 4133) entPhysicalTable.

The ceAssetTable contains an entry (ceAssetEntry) for each physical component on the router. Each entry provides information about the component. The component information includes:

- Orderable part number
- Serial number
- Hardware revision
- Manufacturing assembly number
- Manufacturing revision.

Most physical components are programmed with a standard Cisco-generic ID PROM value that specifies asset information for the component. If possible, the MIB accesses the component's ID PROM information.

Note The ENTITY-MIB (RFC 4133) contains all the objects defined under the CISCO-ENTITY-ASSET-MIB. Thus, you can use the ENTIITY-MIB (RFC 4133) instead of the CISCO-ENTITY-ASSET-MIB.

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.

Note Prior to RLS3 release, CPU entity was modeled for CISCO-ENTITY-EXT-MIB. This behavior has now changed and the RP Module entity is modeled for this MIB instead of CPU entity.

Note ASR1000 RP2 supports 64-bit architecture. The ceExtProcessorRam object of CISCO-ENTITY-EXT-MIB supports only 32 bit values. When RP module contains memory more than 4GB, this object returns incorrect value. New objects will be added to provide 64-bit support for this MIB in Release 4.

MIB Constraints

Only the active RP processor is supported in Cisco ASR 1000 Series Router. The standby RP and SIP processors are not managed in this MIB.

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

Table 3-41 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 1000 Series Routers 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. This MIB is applicable to Cisco ASR 1000 Series SPA interface processor (SIP) and shared port adapter (SPA) modules for this release.

Note When RP switchover is caused by the zone failure (when both power supplies in the zone fail) in the active RP. No notification is sent for the modules in the failure zone. The zone failure can be identified by the status of the power supply. P0 and P1 are in one zone, and P2 and P3 are in the other zone.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-ENTITY-FRU-CONTROL-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, CISCO-ENTITY-FRU-CONTROL-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

MIB Constraints

Table 3-42 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-ENTITY-FRU-CONTROL-MIB.

Table 3-42 CISCO-ENTITY-FRU-CONTROL-MIB Constraints

MIB Object	Notes
cefcModuleTable	
• cefcModuleAdminStatus	Read only. Always enabled(1) for harddisk and USB.

Table 3-42 CISCO-ENTITY-FRU-CONTROL-MIB Constraints (continued)

MIB Object	Notes
• cefcModuleOperStatus	The following values are supported: • unknown(1) • ok(2) • boot(5) • failed(7) • dormant(12) • outOfServiceAdmin(13) Always ok(2) for harddisk and USB.
• cefcModuleResetReason	Implemented for SPA Modules only.
• cefcModuleLastClearConfigTime	Not implemented.
• cefcModuleResetReasonDescription	Not implemented.
• cefcModuleStateChangeReasonDescr	Not implemented.
cefcFRUPowerSupplyGroupTable	Not implemented.
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 and Harddisk.

The Cisco ASR 1002 Router behavioral changes for RP, SIP, and SPA 0/0:

- The RP, SIP, and SPA 0/0 are fixed on the Cisco ASR 1002 chassis and CISCO-ENTITY-FRU-CONTROL-MIB does not have entries for these modules. You can use CISCO-ENTITY-ALARM-MIB to monitor these modules.
- When the status of these modules is changed, the cefcModuleStatusChange trap is generated with the entity physical status of the module.
- When the status of SIP module is changed to down/up, cefcFRURemoved/cefcFRUInserted trap is generated for SPA 0/0 module.

Note The RP, FP, and SIP can not be removed from the ASR1002-F chassis.

Note The CISCO-ENTITY-FRU-CONTROL-MIB is supported on the ASR 1001 chassis.

CISCO-ENTITY-PERFORMANCE-MIB

The CISCO-ENTITY-PERFORMANCE-MIB defines objects to monitor the performance of the Crypto ASIC module of the Extended Service Platform (ESP). Performance monitoring includes utilization of resources and I/O rate for packets and bytes.

MIB Constraints

Table 3-43 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-ENTITY-PERFORMANCE-MIB. These constraints are applicable only for the Crypto ASIC module.

Table 3-43 CISCO-ENTITY-PERFORMANCE-MIB Constraints

MIB Object	Notes
cepEntityTable	Not supported.
cepConfigTable	Read only.
• CiscoEntPerfType	These MIB object values are supported: • utilization(1) • packetInputRate(5) – Mapped to Decrypt Packet Rate (DPR.) • packetOutputRate(6) – Mapped to Encrypt Packet Rate (EPR).
• cepConfigRisingThreshold	Read only.
• cepConfigFallingThreshold	Read only.
• cepConfigThresholdNotifEnabled	Read only.
cepEntityIntervalTable	Supports performance monitoring every 15 minutes.
cepIntervalStatsTable	Supports interval value, fifteenMinutes (3).
cepPerfThreshFallingEvent	Not supported.
cepPerfThreshRisingEvent	Not supported.
cepThresholdNotifEnabled	Read only.

CISCO-ENTITY-QFP-MIB

The CISCO-ENTITY-QFP-MIB defines objects to manage Quantum Flow Processors (QFP) listed as entPhysicalClass attribute in the entPhysicalTable of ENTITY-MIB.. The Quantum Flow Processors (QFP) technology control functions such as packet forwarding via fully integrated and programmable networking chipsets. This MIB module contains objects to monitor various QFP statistics such as system state, processor utilization, and memory.

The processor utilization statistics comprise these attributes:

- Input—Communication channel where packets arrive on the QFP.
- Output—Communication channel where packets exit the QFP.
- Priority—Indicates that the processing priority for the packet is high.
- Non-Priority—Indicates that the processing priority for the packet is low.
- Processing Load—Indicates the percentage of time spent forwarding packets.

Note QFP entities from an inactive or standby FP are not monitored.

Note For ESP100 or ESP200, the processing load reports the average value for the different CPP subdevs, and for other statistics like pps (packets per second) and bps (bytes per second), SNMP reports the sum of the individual values for the different CPP subdevs.

MIB Tables

Table 3-44 lists the tables in CISCO-ENTITY-QFP-MIB.

Table 3-44 CISCO-ENTITY-QFP-MIB Tables

MIB Table	Description
ceqfpSystemTable	Contains the QFP system information for each QFP physical entity. A separate row is created for each QFP physical entity when a physical entity supporting the QFP system information is detected. If a physical entity supporting the QFP system information is removed, the corresponding row is deleted from the table.
ceqfpUtilizationTable	Contains the utilization statistics for each QFP physical entity. A separate row is created for each QFP physical entity when a physical entity supporting the QFP system information is detected. If a physical entity supporting the QFP system information is removed or the utilization statistics are not received for a specific interval, the corresponding row is deleted from the table. The interval to wait before deleting an entry from this table depends on the supporting device.
ceqfpMemoryResourceTable[1]	Contains the memory resources statistics for each QFP physical entity. A separate row is created for each QFP physical entity when a physical entity supporting the QFP system information is detected. If a physical entity supporting the QFP system information is removed or the memory resource statistics are not received for a specific interval, the corresponding row is deleted from the table.
ciscoEntityQfpSystemGroup	Contains objects related to QFP system information.
ciscoEntityQfpUtilizationGroup	Contains objects related to QFP utilization information.
ciscoEntityQfpMemoryResourceGroup	Contains objects related to QFP memory resource information.
ciscoEntityQfpNotifGroup	Contains QFP notification such as memory resource crossing threshold.
ciscoEntityQfpMemoryResNotifGroup	Contains the QFP memory resource notification control object.

[1] The physical DRAM memory resource is logically divided into DRAM and IRAM in the CLI, but the ceqfpMemoryResourceTable table would show the aggregate of DRAM and IRAM data. The IRAM memory is secondary and is used when DRAM memory is exhausted . The notification is generated whenever the threshold exceeds or subcedes the aggregated value.

MIB Constraints

Table 3-45 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-ENTITY-QFP-MIB.

Table 3-45 CISCO-ENTITY-QFP-MIB Constraints

MIB Object	Notes
ciscoEntityQfpMemoryResourceGroup	
• ceqfpMemoryResRisingThreshold	Read only.
• ceqfpMemoryResFallingThrehold	Read only.

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 SPA modules and transceiver modules inserted in the SPAs. This MIB allows you to monitor sensor values and thresholds on sensors that are discovered by the ENTITY-MIB.

Note The CISCO-ENTITY-SENSOR-MIB is supported on the Cisco ASR 1001 chassis.

Note Effective from Cisco IOS Release 15.1(3)S, the CISCO-ENTITY-SENSOR-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the CISCO-ENTITY-SENSOR-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

MIB Constraints

Table 3-46 lists the constraints that the Cisco ASR 1000 Series Router places on the CISCO-ENTITY-SENSOR-MIB.

Table 3-46 CISCO-ENTITY-SENSOR-MIB Constraints

MIB Object	Notes
entSensorValueTable	
• entSensorMeasuredEntity	Implemented for all sensors except for SPA and transceiver sensors.
entSensorThresholdTable	Not implemented for voltage sensors on RP, FP, and CC.
• entSensorThresholdRelation	Read only.
• entSensorThresholdSeverity	Read only.
• entSensorThresholdValue	Read only.

Note The MIB object entSensorThresholdEvaluation for SPA module is not supported, as the SPA sensor monitoring is not supported and the sensor value is updated only on demand. Hence for SPA sensors, you can compare the entSensorValue retrieved from the agent with thresholds to obtain the entSensorThresholdEvaluation.

MIB Usage Values for Cisco Transceivers

The table in this section lists each type of sensor's value represented in the entSensorValueTable and the entSensorThresholdTable.

Table 3-47 lists CISCO-ENTITY-SENSOR-MIB sensor objects and their usage values for Cisco ASR 1000 Series Routers transceivers in the entSensorValueTable.

Table 3-47 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco 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).
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).
Tx Laser Current Sensor	
• entSensorType	amperes(5)
• entSensorScale	milli(8)
• entSensorPrecision	0
• entSensorStatus	ok(1)
• entSensorValue	Reports most recent measurement seen by the sensor.

Table 3-47 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco Transceivers (continued)

MIB Sensor Object	Notes
• 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).
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).

Note The RPs, FPs, SIPs, 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 1000 Series Routers components. The OIDs in this MIB are used by the entPhysicalTable of the ENTITY-MIB as values for the entPhysicalVendorType field in the entPhysicalTable. Each OID uniquely identifies a type of physical entity:

- Chassis
- Optical Services Module
- RP Module
- FP or ESP Module
- SPAs
- SIPs

Note In ASR1002-F, the CC, FP and ESP are fixed in the Chassis and can not be removed. At an instance, only one SPA bay is accessible.

Note The CISCO-ENTITY-VENDORTYPE-OID-MIB is also supported on the ASR1013 and the Cisco ASR 1001 chassis.

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-ENTITY-VENDORTYPE-OID-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the CISCO-ENTITY-VENDORTYPE-OID-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

CISCO-ETHERLIKE-EXT-MIB

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

Note Effective from Cisco IOS Release 15.3(1)S, the CISCO-ETHERLIKE-EXT-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card.

MIB Constraints

Table 3-48 lists the constraint that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-ETHERLIKE-EXT-MIB.

Table 3-48 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 3-49 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-EVC-MIB.

Table 3-49 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 3-50 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-FLASH-MIB.

Table 3-50 CISCO-FLASH-MIB Constraints

MIB Object	Notes
ciscoFlashDeviceTable • ciscoFlashDeviceInitTime • ciscoFlashPhyEntIndex	 Not Implemented. Not Implemented.
ciscoFlashPartitionTable • ciscoFlashPartitionFileCount • ciscoFlashPartitionChecksumAlgorithm • ciscoFlashPartitionUpgradeMethod • ciscoFlashPartitionNeedErasure • ciscoFlashPartitionFileNameLength	 Not Implemented. Not Implemented. Not Implemented. Not Implemented. Not Implemented.

ciscoFlashFileTable
• ciscoFlashFileChecksum
• ciscoFlashFileType
	
	Not Implemented.
	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 RPs are up and running, entities for standby usb flash and Flash disk are not populated for CISCO-FLASH-MIB. Compact Flash is not supported in ASR series Routers. So, it wont be modelled in CISCO-FLASH-MIB.

Note Once the file is copied successfully via tftp, it takes atleast 50 secs to reflect the correct file size in ciscoFlashFileSize object.

CISCO-FRAME-RELAY-MIB

The CISCO-FRAME-RELAY-MIB contains Frame Relay information that is specific to Cisco products or that is missing from RFC 1315.

MIB Constraints

Table 3-51 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-FRAME-RELAY-MIB. Objects that are not listed in the table are implemented as defined in the MIB.

Note Frame Relay Switched Virtual Circuits (SVCs) are not currently supported in Cisco ASR 1000 Series Routers.

Table 3-51 CISCO-FRAME-RELAY-MIB Constraints

MIB Object	Notes
cfrCircuitTable	
• cfrCircuitType	Supported value is pvc(1).
cfrExtCircuitTable	
• cfrExtCircuitMinThroughputOut	Supported for QoS. Otherwise value is 0.
• cfrExtCircuitMinThroughputIn	Supported for QoS. Otherwise value is 0.
• cfrExtCircuitShapeByteLimit	Supported for QoS. Otherwise value is 0.
• cfrExtCircuithapeInterval	Supported for QoS. Otherwise value is 0.
• cfrExtCircuitShapeByteIncrement	Supported for QoS. Otherwise value is 0.
• cfrExtCircuitShapeActive	Supported for QoS. Otherwise value is 0.
• cfrExtCircuitShapeAdapting	Supported for QoS. Otherwise value is 0.
cfrMapTable	

Table 3-51 CISCO-FRAME-RELAY-MIB Constraints (continued)

MIB Object	Notes
• cfrMapType	Values are: • static(1) • dynamic(2)
cfrSvcTable	Not implemented.

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.

Note This MIB is currently not supported for broadband configurations.

CISCO-IETF-BFD-MIB

The CISCO-IETF-BFD-MIB contains managed object definitions for the Bidirectional Forwarding Detection (BFD) Protocol. BFD is a protocol that detects faults in the bidirectional path between two forwarding engines, including interfaces, data links, and to the extent possible, the forwarding engines themselves, with potentially very low latency. It operates independently of media, data protocols, and routing protocols.

Note The CISCO-IETF-BFD-MIB is based on the draft-ietf-bfd-mib-07.txt internet draft.

Following is the support information on the Virtual Routing and Forwarding (VRF) context for the MIB:

- The CISCO-IETF-BFD-MIB supports IPv4 and IPv6 in the non-VRF context.
- The CISCO-IETF-BFD-MIB supports IPv4 in the VRF context, and does not support IPv6 in the VRF context.

CISCO-IETF-FRR-MIB

The CISCO-IETF-FRR-MIB contains managed object definitions for MPLS Fast Reroute (FRR).

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-NAT-MIB

The CISCO-IETF-NAT-MIB contains objects for Network Address Translation (NAT) operations on the router, as defined in RFC 3022. The MIB inclued objects containing NAT configuration, NAT bindings, and run-time statistics.

The MODULE-IDENTITY for the CISCO-IETF-NAT-MIB is ciscoIetfNatMIB, and its top-level OID is 1.3.6.1.4.1.9.10.77 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIetfNatMIB).

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 Pseudo Wire (PW) emulation of ATM over Packet Switched Networks (PSN).

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-IETF-PW-ATM-MIB is supported on SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-52 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-IETF-PW-ATM-MIB.

Table 3-52 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 pseudo wire services over a Packet Switched Network (PSN).

MIB Constraints

Table 3-53 lists the constraints that the Cisco ASR 1000 Series Router place on the objects in the CISCO-IETF-PW-ENET-MIB.

Table 3-53 CISCO-IETF-PW-ENET-MIB Constraints

MIB Object	Notes
cpwVcEnetMplsPriMappingTable	Not supported.
cpwVcEnetStatsTable	Not supported.

CISCO-IETF-PW-FR-MIB

The CISCO-IETF-PW-FR-MIB contains the network management objects defined for FRoPW services over a PSN.

CISCO-IETF-PW-MIB

The CISCO-IETF-PW-MIB contains managed object definitions for PW operation.

Note Effective from Cisco IOS Release 15.1(3)S, the CISCO-IETF-PW-MIB is supported on the SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-54 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-IETF-PW-MIB.

Table 3-54 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.

Table 3-54 CISCO-IETF-PW-MIB Constraints

MIB Object	Notes
• 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.
• 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.

Note Effective from Cisco IOS Release 15.1(3)S, the CISCO-IETF-PW-MPLS-MIB is supported on the SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

MIB Constraints

Table 3-55 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-IETF-PW-MPLS-MIB.

Table 3-55 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 pseudo-wires over packet-switching networks (PSN). The SPA-1XOC3-ATM-V2 and SPA-3XOC3-ATM-V2 do not support CEM (Circuit Emulation). Therefore. this MIB is not supported for these hardware.

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).

Note Effective from Cisco IOS Release 15.1(3)S, CISCO-IF-EXTENSION-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the CISCO-IF-EXTENSION-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

MIB Constraints

Table 3-56 lists constraints that the Cisco ASR 1000 Series Router places on the object in CISCO-IF-EXTENSION-MIB

Table 3-56 CISCO-IF-EXTENSION-MIB Constraints

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

Notes

Some objects defined in cieIfPacketStatsTable and cieIfInterfaceTable are applicable to physical interfaces only. 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 image.

CISCO-IMAGE-LICENSE-MGMT-MIB

The CISCO-IMAGE-LICENSE-MGMT-MIB contains objects to control the management level of the IOS image on a device. Cisco licensing mechanism provides flexibility to run a device at different image levels. This mechanism is referred to as image-level licensing. Image-level licensing leverages the universal image-based licensing solution. A universal image containing all levels of a software package is loaded on to the device. During startup, the device determines the highest level of license and loads the corresponding software features or subsystems.

CISCO-IP-LOCAL-POOL-MIB

The CISCO-IP-LOCAL-POOL-MIB contains objects that provide a network manager with information related to the local IP address pools. This MIB provides configuration and statistics reflecting the allocation of local IP pools. Each entry provides information about a particular local IP pool, including the number of free and used addresses.

The SNMP agent does not have to be configured in any special way for CISCO-IP-LOCAL-POOL-MIB objects to be available to the network management system. You can configure the SNMP agent to send the ciscoIpLocalPoolInUseAddrNoti notification to a particular host using the **snmp-server host** *ip-address community-name* **iplocalpool** command.

The ciscoIpLocalPoolInUseAddrNoti notification is enabled:

- Through SNMP by using the cIpLocalPoolNotificationsEnable object
- Using the **snmp-server enable traps ip local pool** CLI configuration

CISCO-IPMROUTE-MIB

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

CISCO-IPSEC-FLOW-MONITOR-MIB

The CISCO-IPSEC-FLOW-MONITOR-MIB allows monitoring of the structures in IPsec-based virtual private networks.

CISCO-IPSEC-MIB

The CISCO-IPSEC-MIB models the Cisco implementation-specific attributes of a Cisco entity that implements IPsec.

CISCO-IPSEC-POLICY-MAP-MIB

The CISCO-IPSEC-POLICY-MAP-MIB contains objects that supplement the proposed IETF standards for IPsec VPNs. In particular, this MIB maps dynamically instantiated IPsec protocol structures (such as tunnels and security associations) to the policy entities that created them (such as policy definitions, crypto maps, and transforms).

The MODULE-IDENTITY for the CISCO-IPSEC-POLICY-MAP-MIB is ciscoIpSecPolMapMIB, and its top-level OID is 1.3.6.1.4.1.9.9.172 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIpSecPolMapMIB).

MIB Constraints

This MIB is supported only in Cisco IOS software images that support DES encryption (-k8- or -k9-).

CISCO-IP-TAP-MIB

The CISCO-IP-TAP-MIB manages Cisco intercept feature for IP. This MIB is used along with CISCO-TAP2-MIB to intercept IP traffic.

CISCO-IP-URPF-MIB

The CISCO-IP-URPF-MIBcontains objects that allow users to specify a Unicast Reverse Path Forwarding (URPF) drop-rate threshold on interfaces of a managed device, which when exceeded, a SNMP notification is sent. It includes objects specifying global (to a managed device as a whole) and per-interface drop counts and drop rates, and also generates traps based on the drop rate exceeding a configureable per-interface threshold.

MIB Constraints

Table 3-57 lists the constraints that Cisco ASR 1000 Series Router places on the CISCO-IP-URPF-MIB.

Table 3-57 CISCO-IP-URPF-MIB Constraints

MIB Object	Notes
cipUrpfIfMonTable	Entries in this tables are present when URPF is enabled on an interface. They are not available when the interface is removed or if RPF is disabled on the interface.
cipUrpfIfConfTable	Entries in this tables are present when URPF is enabled on an interface. They are not available when the interface is removed or if RPF is disabled on the interface.

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-LICENSE-MGMT-MIB

The CISCO-LICENSE-MGMT-MIB contains objects to manage the licenses on a system. The licensing mechanism provides flexibility to enforce licensing for various features in the system. These are the different kinds of licenses:

- NODE LOCKED LICENSE
- NON-NODE LOCKED LICENSE
- METERED LICENSE
- EVALUATION LICENSE
- RIGHT TO USE (RTU) LICENSE
- EXTENSION LICENSE
- GRACE PERIOD LICENSE
- COUNTED LICENSE
- UNCOUNTED LICENSE
- IMAGE LEVEL LICENSING
- FEATURE LEVEL LICENSING

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-NBAR-PROTOCOL-DISCOVERY-MIB

The CISCO-NBAR-PROTOCOL-DISCOVERY-MIB provides SNMP support for Network-Based Application Recognition (NBAR), including enabling and disabling protocol discovery on a per-interface basis, and configuring the traps that are generated when certain events occur. You can also display the current NBAR configuration and run-time statistics.

Note The MODULE-IDENTITY for the CISCO-NBAR-PROTOCOL-DISCOVERY-MIB is ciscoNbarProtocolDiscoveryMIB, and its top-level OID is 1.3.6.1.4.1.9.9.244 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoNbarProtocolDiscoveryMIB).

Note The cnpdTopNConfigTable and cnpdTopNStatsTable tables do not have details for the protocol "unknown".

CISCO-NETFLOW-MIB

The CISCO-NETFLOW-MIB provides a simple and easy method to get NetFlow cache information, the current NetFlow configuration, and statistics.

MIB Constraints

Table 3-58 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-NETFLOW-MIB.

Table 3-58 CISCO-NETFLOW-MIB Constraints

MIB Object	Notes
cnfCICacheEnable	The following values are not supported: • destinationOnly(6) • sourceDestination(7) • fullFlow(8) • expBgpPrefix(23)

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.

MIB Constraints

Table 3-59 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-NTP-MIB.

Table 3-59 CISCO-NTP-MIB Constraints

MIB Object	Notes
cntpSysLeap	Read only.
cntpSysStratum	Read only.

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 for OSPF-MIB IETF draft draftietf-ospf-mib-update-05.txt in addition to support for OSPF Sham link.

CISCO-PIM-MIB

The CISCO-PIM-MIB defines Cisco-specific objects and variables for managing Protocol Independent Multicast (PIM) 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-PPPOE-MIB

The CISCO-PPPOE-MIB contains objects to manage Point-to-Point Protocol over Ethernet (PPPoE) sessions. These objects represent PPPoE sessions at the system and virtual channel (VC) level.

MIB Constraints

Table 3-60 lists the constraints that the Cisco ASR 1000 Series Router places on the objects in the CISCO-PPPOE-MIB.

Table 3-60 CISCO-PPPOE-MIB Constraints

MIB Object	Notes
cPppoeSystemMaxAllowedSessions	Read only.
cPppoeSystemThresholdSessions	Read only.
cPppoeVcCfgTable • cPppoeVcEnable	 Read only.
cPppoeVcSessionsTable • cPppoeVcMaxAllowedSessions • cPppoeVcExceededSessionErrors	 Read only. Read only.

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 as an estimate only)

MIB Constraints

Table 3-61 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-PROCESS-MIB.

Table 3-61 CISCO-PROCESS-MIB Constraints

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

Note The Cisco ASR1000 RP2 supports 64-bit architecture. Effective from Cisco IOS Release 15.2(4)S onwards, the CISCO-PROCESS-MIB supports 64-bit architecture.

Note The RP2 contains 2 physical CPUs, but the CPUs are not monitored separately. The monitoring the CPU utilization is the aggregate result of both the CPUs. Hence, the cpmCPUTotalTable object contains only one entry for RP 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 cpmVirtualProcessTable is not populated on ESP since the IOS daemon is not running on ESP.

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

Table 3-62 lists the support matrix for the CISCO-PROCESS-MIB cpmCPUTotalTable object.

Table 3-62 Support-Matrix for cpmCPUTotalTable

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

Table 3-63 lists the support matrix for cpmProcessTable and cpmProcessExtRevTable for ESP CPU.

Table 3-63 Support Matrix for cpmProcessTable and cpmProcessExtRevTable for ESP CPU

cpmProcessTable and cpmProcessExtRevTable Objects	Processes[Process Name: cman_fp, fman_fp_image, hman]
cpmProcessPID	Yes
cpmProcessName	Yes
cpmProcessuSecs	No
cpmProcessTimeCreated	Yes
cpmProcessAverageUSecs	Yes
cpmProcExtMemAllocatedRev	Yes
cpmProcExtMemFreedRev	No
cpmProcExtInvokedRev	No
cpmProcExtRuntimeRev	No
cpmProcExtUtil5SecRev	No
cpmProcExtUtil1MinRev	No
cpmProcExtUtil5MinRev	No
cpmProcExtPriorityRev	Yes
cpmProcessType	No
cpmProcessRespawn	No
cpmProcessRespawnCount	No
cpmProcessRespawnAfterLastPatch	No
cpmProcessMemoryCore	No
cpmProcessLastRestartUser	No
cpmProcessTextSegmentSize	No
cpmProcessDataSegmentSize	No
cpmProcessStackSize	No
cpmProcessDynamicMemorySize	No

Table 3-64 lists the support matrix for the CISCO-PROCESS-MIB cpmProcessTable and cpmProcessExtRevTable objects for RP CPU.

Table 3-64 Support Matrix for the cpmProcessTable and the cpmProcessRevExtTable for RP CPU

cpmProcessTable and cpmProcessRevExtTable Objects	IOSD Process [Process Name: ppc_linux_iosd-]	Other Process [Process Name: Cmand, hman, imand]
cpmProcessName	Yes	Yes
cpmProcessuSecs	No	No
cpmProcessTimeCreated	Yes	Yes
cpmProcessAverageUSecs	Yes	Yes

Table 3-64 Support Matrix for the cpmProcessTable and the cpmProcessRevExtTable for RP CPU

cpmProcessTable and cpmProcessRevExtTable Objects	IOSD Process [Process Name: ppc_linux_iosd-]	Other Process [Process Name: Cmand, hman, imand]
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 3-65 lists the support matrix for the CISCO-PROCESS-MIB cpmProcessTable and cpmProcessExtRevTable objects for CC CPU.

Table 3-65 Support Matrix for the cpmProcessTable and the cpmProcessExtRevTable for CC CPU

cpmProcessTable & cpmProcessExtRevTable Objects	SPA IOS Process	Other Process [Process Name: cmcc, hman, imccd]
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

Table 3-65 Support Matrix for the cpmProcessTable and the cpmProcessExtRevTable for CC CPU

cpmProcessTable & cpmProcessExtRevTable Objects	SPA IOS Process	Other Process [Process Name: cmcc, hman, imccd]
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 3-66 lists the support matrix for the CISCO-PROCESS-MIB cpmVirtualProcessTable object.

Table 3-66 Support Matrix for the cpmVirtualProcessTable

cpmVirtualProcessTable Objects	Process running under Active RP IOSD Process	Process running under CC SPA IOS Process
cpmVirtualProcessName	Yes	Yes
cpmVirtualProcessUtil5Sec	Yes	Yes
cpmVirtualProcessUtil1Min	Yes	Yes
cpmVirtualProcessUtil5Min	Yes	Yes
cpmVirtualProcessMemAllocated	Yes	Yes
cpmVirtualProcessMemFreed	Yes	Yes
cpmVirtualProcessInvokeCount	Yes	Yes
cpmVirtualProcessRuntime	Yes	Yes

Table 3-67 lists the threshold values for committed memory.

Table 3-67 Threshold Values for Committed Memory

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
cc	10G	512	95	100
cc	10G	1024	95	100
cc	40G	1024	95	100
fp	5G	1024	90	95
fp	10G	1024	90	95

Table 3-67 Threshold Values for Committed Memory (continued)

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
fp	20G	2048	90	95
fp	20G	4096	90	95
fp	10G	2048	90	95
fp	40G	8192	90	95
fp	40G	16384	90	95
fp	80G	16384	90	95
fp	160G	32768	90	95
rp	RP1	2048	90	95
rp	RP1	4031	90	95
rp	RP1	4096	90	95
rp	1RU	4096	300	310
rp	1RU	8192	300	310
rp	1RU	16384	300	310
rp	2RU	2048	90	95
rp	2RU	4031	90	95
rp	2RU	4096	90	95
rp	RP2	8192	90	95
rp	RP2	16384	90	95
rp	RSP	2048	300	310

Table 3-68 lists the threshold values for average load conditions at 1 minute:

Table 3-68 Threshold Values for Average Load Conditions at 1 Minute

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
cc	10G	512	5	8
cc	10G	1024	5	8
cc	40G	1024	5	8
fp	5G	1024	5	8
fp	10G	1024	5	8
fp	20G	2048	5	8
fp	20G	4096	5	8
fp	10G	2048	5	8
fp	40G	8192	5	8
fp	40G	16384	5	8
fp	80G	16384	5	8
fp	160G	32768	5	8

Table 3-68 Threshold Values for Average Load Conditions at 1 Minute (continued)

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
rp	RP1	2048	5	8
rp	RP1	4031	5	8
rp	RP1	4096	5	8
rp	1RU	4096	8	12
rp	1RU	8192	8	12
rp	1RU	16384	8	12
rp	2RU	2048	5	8
rp	2RU	4031	5	8
rp	2RU	4096	5	8
rp	RP2	8192	5	8
rp	RP2	16384	5	8
rp	RSP	2048	8	12

Table 3-69 lists the threshold values for average load conditions at 5 minutes:

Table 3-69 Threshold Values for Average Load Conditions at 5 Minutes

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
cc	10G	512	5	8
cc	10G	1024	5	8
cc	40G	1024	5	8
fp	5G	1024	5	8
fp	10G	1024	5	8
fp	20G	2048	5	8
fp	20G	4096	5	8
fp	10G	2048	5	8
fp	40G	8192	5	8
fp	40G	16384	5	8
fp	80G	16384	5	8
fp	160G	32768	5	8
rp	RP1	2048	5	8
rp	RP1	4031	5	8
rp	RP1	4096	5	8
rp	1RU	4096	8	12
rp	1RU	8192	8	12
rp	1RU	16384	8	12

Table 3-69 Threshold Values for Average Load Conditions at 5 Minutes (continued)

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
rp	2RU	2048	5	8
rp	2RU	4031	5	8
rp	2RU	4096	5	8
rp	RP2	8192	5	8
rp	RP2	16384	5	8
rp	RSP	2048	8	12

Table 3-70 lists the threshold values for average load conditions at 15 minutes:

Table 3-70 Threshold Values for Average Load Conditions at 15 Minutes

Board Type	Subtype	Total Available Memory	Warning Values(%)	Critical values(%)
cc	10G	512	5	8
cc	10G	1024	5	8
cc	40G	1024	5	8
fp	5G	1024	5	8
fp	10G	1024	5	8
fp	20G	2048	5	8
fp	20G	4096	5	8
fp	10G	2048	5	8
fp	40G	8192	5	8
fp	40G	16384	5	8
fp	80G	16384	5	8
fp	160G	32768	5	8
rp	RP1	2048	5	8
rp	RP1	4031	5	8
rp	RP1	4096	5	8
rp	1RU	4096	10	15
rp	1RU	8192	10	15
rp	1RU	16384	10	15
rp	2RU	2048	5	8
rp	2RU	4031	5	8
rp	2RU	4096	5	8
rp	RP2	8192	5	8
rp	RP2	16384	5	8
rp	RSP	2048	10	15

CISCO-PRODUCTS-MIB

The CISCO-PRODUCTS-MIB lists the object identifiers (OIDs) assigned to the Cisco hardware platforms. CISCO ASR1006, ASR1004, ASR1002, ASR1002-F, ASR1001, and ASR1013 OIDs are supported.

CISCO-QINQ-VLAN-MIB

The CISCO-QINQ-VLAN-MIB describes configuration and monitoring capabilities relating to 802.1QinQ interfaces.

MIB Constraints

Table 3-71 lists the constraints that the Cisco ASR 1000 Series Routers places on the objects in the CISCO-QINQ-VLAN-MIB.

Table 3-71 CISCO-QINQ-VLAN-MIB Constraints

MIB Object	Notes
cqvTerminationTable • cqvTerminationPeEncap • cqvTerminationRowStatus	 Implemented as Read only. Implemented as Read only.
cqvTranslationTable	Not supported.

CISCO-RADIUS-EXT-MIB

The CISCO-RADIUS-EXT-MIB contains MIB objects used for managing the RADIUS authentication and accounting statistics.

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-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 3-72 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 3-72 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-RTTMON-MIB.

Table 3-72 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	

Table 3-72 CISCO-RTTMON-MIB Constraints (continued)

MIB Object	Notes
• 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-SLB-EXT-MIB

The CISCO-SLB-EXT-MIB contains extensions to the Cisco server load-balancing (SLB) MIB (CISCO-SLB-MIB). Server load balancing enables the router to balance the processing of packets and connections from a number of other devices, such as real servers, firewalls, or caches. An SLB device determines how to handle incoming frames and connections according to the contents of the incoming data and various configuration options.

CISCO-SLB-MIB

The CISCO-SLB-MIB contains objects to manage server load-balancing (SLB) managers, such as those provided by the Cisco IOS SLB product. The MIB includes objects for the manager-side implementation of the Dynamic Feedback Protocol (DFP), which is used to obtain information about servers.

CISCO-SESS-BORDER-CTRLR-CALL-STATS-MIB

The CISCO-SESSION-BORDER-CONTROLLER-CALL-STATS-MIB defines the statistics information for Session Border Controller application. The statistic information is of two types:

- Call statistics
- Media statistics

CISCO-SESS-BORDER-CTRLR-EVENT-MIB

The CISCO-SESS-BORDER-CTRLR-EVENT-MIB defines the SNMP notifications, events, and alarms generated by Session Border Controller application, and sends these notifications to SNMP manager application. The various notification, events, and alarms generated by a SBC application can be:

- Change in the state of a configured SBC service.
- Change in the connection state with an adjacency or a radius server or H.248 controller attached to SBC, CPU or memory congestion, due to a large number of ongoing SIP/H.248 calls.
- Violation in the call policies configured for the current ongoing SIP/H.248 calls, when SBC application receives media (RTP/RTCP) packets from an unknown IP address or port.

CISCO-SESS-BORDER-CTRLR-STATS-MIB

The CISCO-SESS-BORDER-CTRLR-STATS-MIB contains objects to manage the statistics information for the Session Border Controller application. The statistics information is categorized into these types:

- RADIUS Messages Statistics—Represents the statistics of various RADIUS messages for the RADIUS servers with which the client (SBC) shares a secret.
- RF Billing Statistics—Represents the RF billing statistics information, which is used to monitor the messages sent per realm over the IMS Rx interface by the RF billing manager(SBC).
- SIP Statistics—Represents the SIP requests and responses on a SIP adjacency for a specific interval.

MIB Tables

Table 3-73 lists the tables in CISCO-SESS-BORDER-CTRLR-STATS-MIB.

Table 3-73 CISCO-SESS-BORDER-CTRLR-STATS-MIB Tables

MIB Table	Description
csbRadiusStatsTable	Maintains the RADIUS messages for the RADIUS servers.
csbRfBillRealmStatsTable	Maintains the RF billing statistics information.
csbSIPMthdCurrentStatsTable	Contains the total number of SIP request and responses for each SIP method on a given adjacency for a specific interval.
csbSIPMthdHistoryStatsTable	Contains the historical count of SIP requests and responses for each SIP method on a SIP adjacency for the different intervals defined by the csbSIPMthdHistoryStatsInterval object.
csbSIPMthdRCCurrentStatsTable	Contains the SIP method request and response code statistics corresponding to the method and response code combination on a given adjacency for a specific interval.
csbSIPMthdRCHistoryStatsTable	Contains the historical data for the SIP method request and response code statistics corresponding to the method and response code on a given adjacency for a specific interval.

CISCO-SIP-UA-MIB

The CISCO-SIP-UA-MIB manages the Session Initiation Protocol (SIP) User Agents (UA). SIP is an application-layer signalling protocol for creating, modifying, and terminating multimedia sessions with one or more participants. A UA is an application that contains both a User Agent Client (UAC) and a User Agent Server (UAS). A UAC is an application that initiates a SIP request. A UAS is an application that contacts the corresponding user when a SIP request is received and returns a response on behalf of the user.

CISCO-SONET-MIB

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

Note CISCO-SONET-MIB supports SONET traps that are seen when the linestatus, sectionstatus, pathstatus changes, and Notifications are enabled.

MIB Constraints

The following CISCO-SONET-MIB tables are not implemented in the Cisco ASR 1000 Series Routers:

- csConfigTable
- csVTConfigTable
- csAPSConfigTable
- cssTraceTable
- cspTraceTable
- csStatsTable
- cspConfigTable

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

CISCO-SUBSCRIBER-SESSION-MIB

The CISCO-SUBSCRIBER-SESSION-MIB contains objects that describe the subscriber sessions terminated by a Remote Access Service (RAS).

MIB Tables

Table 3-74 lists the tables in CISCO-SUBSCRIBER-SESSION-MIB.

Table 3-74 CISCO-SUBSCRIBER-SESSION-MIB Tables

MIB Table	Description
csubSessionTable	Describes a list of subscriber sessions currently maintained by the system.
csubSessionByTypeTable	Sorts the subscriber sessions first by corresponding subscriber session type, and then by the ifIndex assigned to the corresponding subscriber session.
csubAggStatsTable	Contains sets of aggregated statistics pertaining to subscriber sessions, where each set has a unique scope of aggregation.
csubAggStatsIntTable	Contains aggregated subscriber session performance data collected for every 15-minute measurement intervals.
csubJobTable	Contains the subscriber session jobs submitted by the element management system (EMS) and network management system (NMS).
csubJobMatchParamsTable	Contains subscriber session job parameters that describe the match criteria.
csubJobQueryParamsTable	Contains subscriber session job parameters that describe the query parameters.
csubJobQueueTable	Lists the subscriber session jobs pending in the subscriber session job queue.
csubJobReportTable	Contains the reports corresponding to subscriber session jobs that have *query* as the csubJobType, and *finished* as the csubJobState.

MIB Constraints

Table 3-75 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the CISCO-SUBSCRIBER-SESSION-MIB. Any MIB object that is not listed in this table is implemented as defined in the MIB.

Table 3-75 CISCO-SUBSCRIBER-SESSION-MIB Constraints

MIB Object	Notes
csubSessionByTypeTable	Not implemented.
csubAggStatsIntTable	Not implemented.
csubJobQueueTable	Not implemented.
csubSessionTable	
• csubSessionType	Read only. The pppSubscriber(3), pppoeSubscriber(4), ipInterfaceSubscriber(7), ipPktSubscriber(8), and ipDhcpv4Subscriber(9) types are supported.
• csubSessionAuthenticated	Read only.
• csubSessionCreationTime	Read only.
• csubSessionAvailableIdentities	Read only.

Table 3-75 CISCO-SUBSCRIBER-SESSION-MIB Constraints (continued)

MIB Object	Notes
• csubSessionSubscriberLabel	Read only.
• csubSessionMacAddress	Read only.
• csubSessionNativeVrf	Read only.
• csubSessionNativeIpAddrType	Read only.
• csubSessionNativeIpAddr	Read only.
• csubSessionNativeIpMask	Read only.
• csubSessionDomainVrf	Read only.
• csubSessionPbhk	Read only.
• csubSessionRemoteId	Read only.
• csubSessionCircuitId	Read only.
• csubSessionNasPort	Read only.
• csubSessionDomain	Read only.
• csubSessionUsername	Read only.
• csubSessionAcctSessionId	Read only.
• csubSessionProtocol	Read only. The IP(3) and PPP(5) values are supported.
• csubSessionLocationIdentifier	Read only.
• csubSessionServiceIdentifier	Read only.
• csubSessionLastChanged	Read only.
• csubSessionNativeIpAddrType2	Read only.
• csubSessionNativeIpAddr2	Read only.
• csubSessionNativeIpMask2	Read only.
• csubSessionIpAddrAssignment	Not implemented.
• csubSessionRedundancyMode	Not implemented.
• csubSessionDerivedCfg	Not implemented.
• csubSessionDnis	Not implemented.
• csubSessionMedia	Not implemented.
• csubSessionMlpNegotiated	Not implemented.
• csubSessionServiceName	Not implemented.
• csubSessionDhcpClass	Not implemented.
• csubSessionTunnelName	Not implemented.
csubAggStatsTable	Currently the scope of aggregation is limited to providing the statistics at the RAS level.
• csubAggStatsPendingSessions	Read only.
• csubAggStatsUpSessions	Read only.
• csubAggStatsAuthSessions	Read only.
• csubAggStatsUnAuthSessions	Read only.

Table 3-75 CISCO-SUBSCRIBER-SESSION-MIB Constraints (continued)

MIB Object	Notes
• csubAggStatsLightWeightSessions	Read only.
• csubAggStatsHighUpSessions	Read only.
• csubAggStatsAvgSessionUptime	Read only.
• csubAggStatsAvgSessionRPM	Read only.
• csubAggStatsAvgSessionRPH	Read only.
• csubAggStatsTotalFailedSessions	Read only.
• csubAggStatsTotalUpSessions	Read only.
• csubAggStatsTotalLightWeightSessions	Read only.
• csubAggStatsTotalFlowsUp	Read only.
• csubAggStatsCurrFlowsUp	Read only.
• csubAggStatsRedSessions	Not implemented.
• csubAggStatsThrottleEngagements	Not implemented.
• csubAggStatsTotalCreatedSessions	Not implemented.
• csubAggStatsTotalAuthSessions	Not implemented.
• csubAggStatsTotalDiscSessions	Not implemented.
• csubAggStatsDayCreatedSessions	Not implemented.
• csubAggStatsDayFailedSessions	Not implemented.
• csubAggStatsDayUpSessions	Not implemented.
• csubAggStatsDayAuthSessions	Not implemented.
• csubAggStatsDayDiscSessions	Not implemented.
• csubAggStatsCurrTimeElapsed	Not implemented.
• csubAggStatsCurrValidIntervals	Not implemented.
• csubAggStatsCurrInvalidIntervals	Not implemented.
• csubAggStatsCurrCreatedSessions	Not implemented.
• csubAggStatsCurrFailedSessions	Not implemented.
• csubAggStatsCurrUpSessions	Not implemented.
• csubAggStatsCurrAuthSessions	Not implemented.
• csubAggStatsCurrDiscSessions	Not implemented.
csubJobTable	
• csubJobId	Read only.
• csubJobStatus	The values, Not-In-Service and Not-Ready, are not supported.
• csubJobStorage	Read only.
• csubJobType	Read only.
• csubJobControl	If the job is executing, the *abort* action is ignored.
• csubJobState	Read only.

Table 3-75 CISCO-SUBSCRIBER-SESSION-MIB Constraints (continued)

MIB Object	Notes
• csubJobStartedTime	The sysuptime at the time of job start is measured in timeticks.
• csubJobFinishedTime	The sysuptime at the time of job start is measured in timeticks.
• csubJobFinishedReason	The value *insufficientResources* is returned if a job query is started without sufficient job match parameters.
csubJobMatchParamsTable	
• csubJobMatchParamsEntry	Read only.
• csubJobMatchIdentities	Read only.
• csubJobMatchSubscriberLabel	Read only.
• csubJobMatchMacAddress	Read only.
• csubJobMatchNativeVrf	Read only.
• csubJobMatchNativeIpAddrType	The job search based on IPv6 is not supported.
• csubJobMatchNativeIpAddr	Read only.
• csubJobMatchPbhk	Read only.
• csubJobMatchOtherParams	Not implemented.
• csubJobMatchDomainVrf	Not implemented.
• csubJobMatchRemoteId	Not implemented.
• csubJobMatchCircuitId	Not implemented.
• csubJobMatchNasPort	Not implemented.
• csubJobMatchUsername	Not implemented.
• csubJobMatchAccountingSid	Not implemented.
• csubJobMatchDomain	Not implemented.
• csubJobMatchDnis	Not implemented.
• csubJobMatchMedia	Not implemented.
• csubJobMatchMlpNegotiated	Not implemented.
• csubJobMatchProtocol	Not implemented.
• csubJobMatchServiceName	Not implemented.
• csubJobMatchDhcpClass	Not implemented.
• csubJobMatchTunnelName	Not implemented.
• csubJobMatchDanglingDuration	Not implemented.
csubJobQueryParamsTable	

Table 3-75 CISCO-SUBSCRIBER-SESSION-MIB Constraints (continued)

MIB Object	Notes
• csubJobQueryResultingReportSize	• When the EMS or NMS sets the *jobcontrol* value to *release*, the job and the csubJobQueryResultingReportSize object become invalid. • The csubJobQueryParamsTable is created only when the jobfinished value becomes *normal*.
csubJobReportTable	
• csubJobReportId	Read only.
• csubJobReportSession	Read only.
csubJobFinishedNotifyEnable	Read-write.
csubJobIndexedAttributes	The supported indexed attributes are: • Subscriber Label • Mac Address • IP Address (IPv4 only) • Native VRF • Port-bundle Host Key (PBHK)

CISCO-SYSLOG-MIB

The CISCO-SYSLOG-MIB contains all system log messages generated by the Cisco IOS software. The MIB provides a way to access these syslog messages through SNMP. All Cisco IOS syslog 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 syslog messages and counts related to syslog messages.

Note You can configure the Cisco ASR 1000 Series Routers to send syslog messages to a syslog server.

Note The MIB does not keep track of messages generated from debug commands entered through the command-line interface (CLI).

Note You can enable syslog messages on Cisco ASR 1000 Series Routers by using **logging history debugging** command.

CISCO-UNIFIED-FIREWALL-MIB

The CISCO-UNIFIED-FIREWALL-MIB contains status and performance statistics for Cisco firewall implementation. The ASR 1000 platform only supports the statistics for the zone base firewall.

Note Begining with Cisco IOS Release 3.6, the CISCO-UNIFIED-FIREWALL-MIB is supported on IPv6 networks.

MIB Tables

Table 3-76 lists the tables in CISCO-UNIFIED-FIREWALL-MIB.

Table 3-76 CISCO-UNIFIED-FIREWALL-MIB Tables

MIB Table	Description
cufwConnSummaryTable	Contains information about the connection activity on the firewall for each layer3 and layer 4 protocols. Each entry in the table lists the connection summary of a distinct network protocol.
cufwAppConnSummaryTable	Contians firewall connections information for Layer 7 protocols. Each entry in the table lists the connection summary corresponding to a distinct application protocol.
cufwPolicyConnSummaryTable	Contains firewall connections information for layer3 and layer 4 protocols for each applied policy. Each entry in the table lists the connection summary of a distinct network protocol, configured on the specified target policy on the firewall.
cufwPolicyAppConnSummaryTable	Contains firewall connections information for Layer 7 protocols for each applied policy. Each entry in the table lists the connection summary of a distinct application protocol, configured on the specified target policy on the firewall.
cufwInspectionTable	Contains objects to identify whether or not an application protocol is configured for inspection. It also contains attributes to identify whether or not the specified protocol is currently being verified.
cufwUrlfServerTable	Lists the URL filtering servers configured on the managed devices and corresponding performance statistics.

MIB Constraints

Table 3-77 lists the constraints that the Cisco ASR 1000 Series Router places on CISCO-UNIFIED-FIREWALL-MIB.

Table 3-77 CISCO-UNIFIED-FIREWALL-MIB Constraints

MIB Object	Notes
cufwInspectionTable	Not supported.
cufwUrlfServerTable	Not supported.
cuFwConnectionGlobalsTable	
• cufwConnGlobalNumSetupsAborted	Not supported, default value set to zero.
• cufwConnGlobalNumPolicyDeclined	Not supported, default value set to zero.
• cufwConnGlobalNumResDeclined	Not supported, default value set to zero.

Table 3-77 CISCO-UNIFIED-FIREWALL-MIB Constraints (continued)

MIB Object	Notes
- cufwConnGlobalNumExpired	Not supported, default value set to zero.
- cufwConnGlobalNumAborted	Not supported, default value set to zero.
- cufwConnGlobalNumEmbryonic	Not supported, default value set to zero.
- cufwConnGlobalNumRemoteAccess	Not supported, default value set to zero.
- cufwConnGlobalConnSetupRate1	The number of sessions created in the last minute.
- cufwConnGlobalConnSetupRate5	The number of sessions created in the last five minutes.
cufwConnSummaryTable	
- cufwConnNumSetupsAborted	Not supported, default value set to zero.
- cufwConnNumPolicyDeclined	Not supported, default value set to zero.
- cufwConnNumResDeclined	Not supported, default value set to zero.
- cufwConnNumAborted	Not supported, default value set to zero.
- cufwConnSetupRate1	The number of sessions created in the last minute.
- cufwConnSetupRate5	The number of sessions created in the last five minutes.
cufwAppConnSummaryTable	
- cufwAppConnNumSetupsAborted	Not supported, default value set to zero.
- cufwAppConnNumPolicyDeclined	Not supported, default value set to zero.
- cufwAppConnNumPolicyDeclined	Not supported, default value set to zero.
- cufwAppConnNumAborted	Not supported, default value set to zero.
- cufwAppConnSetupRate1	The number of sessions created in the last minute.
- cufwAppConnSetupRate5	The number of sessions created in the last five minutes.
cufwPolicyConnSummaryTable	
- cufwPolConnNumSetupsAborted	Not supported, default value set to zero.
- cufwPolConnNumPolicyDeclined	Not supported, default value set to zero.
- cufwPolConnNumResDeclined	Not supported, default value set to zero.
- cufwPolConnNumAborted	Not supported, default value set to zero.
cufwPolicyAppConnSummaryTable	
- cufwPolAppConnNumSetupsAborted	Not supported, default value set to zero.
- cufwPolAppConnNumPolicyDeclined	Not supported, default value set to zero.
- cufwPolAppConnNumResDeclined	Not supported, default value set to zero.
- cufwPolAppConnNumAborted	Not supported, default value set to zero.

CISCO-TAP2-MIB

The CISCO-TAP2-MIB manages Cisco intercept feature. This MIB replaces CISCO-TAP-MIB. This MIB defines a generic stream table that contains fields common to all intercept types. Specific intercept filters are defined in the following extension MIBs:

- CISCO-IP-TAP-MIB for IP intercepts
- CISCO-802-TAP-MIB for IEEE 802 intercepts
- CISCO-USER-CONNECTION-TAP-MIB for RADIUS-based user connection intercepts.

MIB Constraints

Table 3-78 lists the constraints that the Cisco ASR 1000 Series Router places on CISCO-TAP2-MIB.

Table 3-78 CISCO-TAP2-MIB Constraints

MIB Object	Notes
cTap2MediationRtcpPort	Not supported.
cTap2MediationRetransmitType	Not supported.
cTap2MediationTransport	Only udp(1) is supported.

CISCO-TAP-MIB

The CISCO-TAP-MIB contains objects to manage Cisco intercept feature.

CISCO-UBE-MIB

The CISCO-UBE-MIB contains objects to manage the Cisco Unified Border Element (CUBE), which is a Cisco IOS Session Border Controller (SBC) that interconnects independent voice over IP (VoIP) and video over IP networks for data, voice, and video transport.

CISCO-USER-CONNECTION-TAP-MIB

The CISCO-USER-CONNECTION-TAP-MIB is a filter MIB that provides the functionality to manage the Cisco intercept feature for user connections. This MIB is used along with the CISCO-TAP2-MIB to intercept and filter user traffic. To create a user connection intercept, an entry named cuctTapStreamEntry is created in the CISCO-USER-CONNECTION-TAP-MIB. This entry contains the filtering information.

CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

The CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB contains VLAN-ID and ifIndex information for each routed virtual LAN (VLAN) interface on the router. A routed VLAN interface is the router interface or subinterface to which you attach the IP address used by the router on the VLAN. The MIB maps each VLAN-ID to an ifIndex, which you can use to access the ipRouteTable to obtain the routing configuration for the routed VLAN interface.

CISCO-VLAN-MEMBERSHIP-MIB

The CISCO-VLAN-MEMBERSHIP-MIB provides management functions for the VLAN membership within the framework of Cisco VLAN Architecture, Version 2.0. The MIB provides information on VLAN Membership Policy Servers used by a device and VLAN membership assignments of non-trunk bridge ports of the device.

CISCO-VPDN-MGMT-MIB

The CISCO-VPDN-MGMT-MIB provides operational information about the Virtual Private Dialup Network (VPDN) feature on the router. You can use the MIB to monitor VPDN tunnel information on the router, but you cannot use the MIB to configure VPDN.

VPDN enables the router to forward Point-to-Point Protocol (PPP) traffic between an Internet service provider (ISP) and a home gateway. The CISCO-VPDN-MGMT-MIB includes several tables that contain VPDN tunneling information:

- cvpdnSystemTable—Provides system-wide VPDN information.
- cvpdnTunnelAttrTable—Provides information about each active tunnel.
- cvpdnSessionAttrTable—Provides information about each active session within each tunnel.
- cvpdnUserToFailHistInfoTable—Provides information about the last failure that occurred for each tunnel user.
- cvpdnTemplateTable—Identifies each VPDN template and indicates the number of active sessions associated with the template. See Table 3-79 for information about template name restrictions and and their effect on SNMP.

MIB Constraints

The CISCO-VPDN-MGMT-MIB contains read-only information. In addition, the MIB objects in Table 3-79 have been deprecated. Although currently supported, their use is being phased out and we recommend that you use the replacement object instead.

Table 3-79 CISCO-VPDN-MGMT-MIB Constraints

MIB Object	Notes
cvpdnTunnelTotal	Replaced by cvpdnSystemTunnelTotal.
cvpdnSessionTotal	Replaced by cvpdnSystemSessionTotal.
cvpdnDeniedUsersTotal	Replaced by cvpdnSystemDeniedUsersTotal.

Table 3-79 CISCO-VPDN-MGMT-MIB Constraints (continued)

MIB Object	Notes
cvpdnTunnelTable	Replaced by cvpdnTunnelAttrTable.
cvpdnTunnelSessionTable	Replaced by cvpdnSessionAttrTable.
cvpdnTemplateTable	SNMP limits the size of VPDN template names to 128 characters. If any template name in the cvpdnTemplateTable exceeds this length, you cannot use an SNMP getmany request to retrieve any table entries. Instead, you must use individual getone requests to retrieve each template name (cvpdnTemplateName) that does not exceed 128 characters.

Note CISCO-VPDN-MGMT-MIB does not support L2TPv3.

CISCO-VOICE-ANALOG-IF-MIB

The CISCO-VOICE-ANALOG-IF-MIB provides the standard configuration, timing parameters, telephony hook, and ring status information on the Cisco Analog Voice interface implementation. This MIB manages the following groups:

- Analog interface general group
- E&M (recEive and transMit) interface group
- FXO (Foreign Exchange Office) interface group
- FXS (Foreign Exchange Station) interface group

Note This MIB is not supported in the ASR 1000 Series Routers.

CISCO-VOICE-COMMON-DIAL-CONTROL-MIB

The CISCO-VOICE-COMMON-DIAL-CONTROL-MIB contains voice-related objects that are common across more than one network encapsulation, such as VoIP, Voice over ATM (VoATM), and Voice over Frame Relay (VoFR).

CISCO-VOICE-DIAL-CONTROL-MIB

The CISCO-VOICE-DIAL-CONTROL-MIB module enhances the IETF Dial Control MIB (RFC2128) by providing the management of voice telephony peers on both a circuit-switched telephony networks and IP data networks.

CISCO-VOICE-IF-MIB

The CISCO-VOICE-IF-MIB manages the common voice-related parameters for both voice analog and Integrated Services Digital Network (ISDN) interfaces.

Note This MIB is not supported in the ASR 1000 Series Routers.

CISCO-VOIP-TAP-MIB

The CISCO-VOIP-TAP-MIB module defines the objects to manage the Intercept feature for Voice over IP (VoIP). This MIB is used along with CISCO-TAP2-MIB to intercept the VoIP control and data traffic.

DIAL-CONTROL-MIB (RFC 2128)

The DIAL-CONTROL-MIB (RFC 2128) contains peer information for demand access.

DS1-MIB (RFC 2495)

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

Note Effective from Cisco IOS Release 15.1(3)S, DS1-MIB is supported on SPA-24CHT1-CE-ATM.

Note DS1-MIB is not supported on SPA-2CHT3-CE-ATM because only the *clear channel T3* mode is supported in Cisco IOS Release 15.1(3)S.

MIB Constraints

Table 3-80 describes the constraints that the Cisco ASR 1000 Series Router places on the objects in the DS1-MIB. For detailed definitions of the MIB objects, see the corresponding MIB.

Table 3-80 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.

Table 3-80 DS1-MIB Constraints (continued)

MIB Object	Notes
• dsx1LineType	Read only.
• dsx1LineCoding	Read only.
• dsx1SendCode	Read only.
• dsx1CircuitIdentifier	Read only.
• dsx1LoopbackConfig	Read only.
• dsx1SignalMode	Read only or SPA-8XCHT1/E1 usage is always none(1).
• dsx1TransmitClockSource	Read only.
• dsx1Fdl	Read only.
• dsx1LoopbackStatus	SPA-8XCHT1/E1 usage: Payload loopbacks are not supported (dsx1NearEndPayloadLoopback, dsx1FarEndPayloadLoopback).
dsx1FracTable	Not implemented.
dsx1FarEndIntervalTable	Not implemented.

DS3-MIB (RFC 2496)

The DS3-MIB(RFC-2496) contains a description of the DS3 and E3 interface objects.

Note Effective from Cisco IOS Release 15.1(3)S, DS3-MIB is supported on SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the DS3-MIB is supported on SPA-8XT3/E3.

MIB Constraints

Table 3-81 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the RFC1407-MIB. Objects that are not listed in the table are implemented as defined in the RFC 1407-MIB.

Table 3-81 DS3-MIB Constraints

MIB Object	Notes
dsx3ConfigTable	
• dsx3LineType	Supported values are: • T3 supports dsx3M23(2) and dsx3CbitParity(4). • E3 supports e3Framed(7) and e3Plcp(8).

Table 3-81 DS3-MIB Constraints (continued)

MIB Object	Notes
• dsx3LineCoding	Read only. Supported values are: • T3 supports dsx3B3ZS(2). • E3 supports e3HDB3(3).
• dsx3SendCode	Read only. Supports only dsx3SendNoCode
• dsx3TransmitClockSource	Supported values are loopTiming(1) and localTiming(2).
• dsx3CircuitIdentifier	Read only.
• dsx3LoopbackConfig	Read only.
dsx3FarEndConfigTable	Not implemented.
dsx3FarEndCurrentTable	Not implemented.
dsx3FarEndIntervalTable	Not implemented.
dsx3FarEndTotalTable	Not implemented.
dsx3FracTable	Not implemented.

Notes

All T3/ATM line cards only support read-only values on all variables.

Currently for the dsx3FracTable to operate, the DS1 layer must be implemented in the ifTable. In this release, this table is shown as not implemented because no rows are instantiated.

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 1000 Series Router chassis and a row for each entity in the chassis. A physical entity may contain other entities. For example, a SIP10 in slot 6 with one SPA 1XOC12 POS-SPA in subslot 6/0 supports the following entities in this SNMP output for SPAs and SIPs, sensors on the SIP, and SPA ports:

```
entPhysicalDescr.1040 = 1-port OC12/STM4 POS Shared Port Adapter
entPhysicalContainedIn.1040 = 1027
entPhysicalDescr.1066 = subslot 0/0 temperature Sensor 0
entPhysicalContainedIn.1066 = 1040
entPhysicalDescr.1067 = subslot 0/0 temperature Sensor 1
entPhysicalContainedIn.1067 = 1040
entPhysicalDescr.1068 = subslot 0/0 temperature Sensor 2
entPhysicalContainedIn.1068 = 1040
entPhysicalDescr.1078 = subslot 0/0 voltage Sensor 0
entPhysicalContainedIn.1078 = 1040
entPhysicalDescr.1079 = subslot 0/0 voltage Sensor 1
entPhysicalContainedIn.1079 = 1040
entPhysicalDescr.1080 = subslot 0/0 voltage Sensor 2
entPhysicalContainedIn.1080 = 1040
entPhysicalDescr.1081 = subslot 0/0 voltage Sensor 3
entPhysicalContainedIn.1081 = 1040
entPhysicalDescr.1091 = subslot 0/0 transceiver container 0
entPhysicalContainedIn.1091 = 1040
entPhysicalDescr.1092 = OC12 SR-1/STM4 MM
entPhysicalContainedIn.1092 = 1091
entPhysicalDescr.1093 = Packet over Sonet
entPhysicalContainedIn.1093 = 1092
entPhysicalDescr.1095 = subslot 0/0 transceiver 0 Temperature Sensor
entPhysicalContainedIn.1095 = 1092
entPhysicalDescr.1096 = subslot 0/0 transceiver 0 Supply Voltage Sensor
entPhysicalContainedIn.1096 = 1092
entPhysicalDescr.1097 = subslot 0/0 transceiver 0 Bias Current Sensor
entPhysicalContainedIn.1097 = 1092
entPhysicalDescr.1098 = subslot 0/0 transceiver 0 Tx Power Sensor
entPhysicalContainedIn.1098 = 1092
entPhysicalDescr.1099 = subslot 0/0 transceiver 0 Rx Power Sensor
entPhysicalContainedIn.1099 = 1092
```

For more information on this MIB, refer Appendix A, “ENTITY-MIB.”

Note The ENTITY-MIB is also supported on the Cisco ASR 1013 and ASR 1001 chassis.

Note Effective from Cisco IOS Release 15.1(3)S, ENTITY-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the ENTITY-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

For the Cisco ASR1000 platform, the entPhysicalParentRelPos are populated with the slot numbers (except for the RP, ESP, and PEM slot numbers) given in the external label. Table 3-82 lists the mapping between external label and entPhysicalParentRelPos.

Table 3-82 Mapping the External Label to the entPhysicalParentRelPos Value

Type	External Label	Value
SIP Container	0 to 5	0 to 5 match the external label.
RP Container	R0 and R1	6 for R0, and 7 for R1.
FP Container	F0 and F1	8 for F0 and 9 for F1.
Power Supply Bay	0 and 1	14 for PEM 0, and 15 for PEM 1.
CPU		Starts from 0.
QFP		Starts from 0.
Crypto ASIC Module of FP		Starts from 0.

The Cisco ASR 1001 Router chassis includes inbuilt RP module, SIP module, SPA module 0/0, IDC modue 0/2, FP or ESP Module, and FanTray Module. Table 3-83 lists the values of the affected MIB table objects in the Cisco ASR 1001 Router:

Table 3-83 Affected MIB Objects in a Cisco ASR 1001 Router

Type	External Label	Value
entPhysicalContainedIn	RP Module	entPhysicalIndex of Chassis.
	ESP Module	entPhysicalIndex of Chassis.
	SIP Module	entPhysicalIndex of Chassis.
	SPA Module 0/0	entPhysicalIndex of SIP Module.
	IDC Module 0/2	entPhysicalIndex of SIP Module.
	FanTray Module	entPhysicalIndex of Chassis.
entPhysicalIsFRU	RP Module	false(2)
	ESP Module	false(2)
	SIP Module	false(2)
	SPA Module 0/0	false(2)
	IDC Module 0/2	false(2)
	FanTray Module	false(2)
entPhysicalParentRelPos	RP Module	6
	ESP Module	8
	SIP Module	0
	SPA Module 0/0	0
	IDC Module 0/2	2
	FanTray Module	0

Table 3-84 lists the fans supported on a Cisco ASR 1000 series Router.

0

Table 3-84 Fans Supported on a Cisco ASR 1000 series Router

Module	Number of Fans
ASR1001 PEM	1
ASR1002/ASR1002-F PEM	2
ASR1004/ASR1006/ASR1013 PEM	3
ASR1001 FanTray Module	7

Table 3-85 lists the variations between the entPhysicalTable values for the hard disk in the RP1 and RP2 modules.

Table 3-85 Variations Between the entPhysicalTable Values

MIB Object	ASR 1000 RP1	ASR 1000 RP2
entPhysicalContainedIn	entPhysicalIndex of RP module.	entPhysicalIndex of hard disk container.
entPhysicalIsFRU	false(2).	true(1).

MIB Constraints

Table 3-86 lists the constraints that the Cisco ASR 1000 Series Routers places on the objects in the ENTITY-MIB.

Table 3-86 ENTITY-MIB Constraints

MIB Object	Notes
entPhysicalSoftwareRev	Supported for RP and SIP Modules.
entPhysicalAssetAlias	Not supported.
entPhysicalAssetId	Not supported for Transceiver Modules, USB and Harddisk. Implemented only as read-write for the following entPhysicalClass entities: • Chassis • Powersupply • Module
entPhysicalHardwareRev	Not implemented for USB and Harddisk.
entPhysicalSerialNum	Implemented as Readonly. Not implemented for USB and Harddisk.
entPhysicalModelName	Not implemented for USB and Harddisk.
entPhysicalMfgName	Not implemented for USB and Harddisk.
entPhysicalUris	Not implemented for USB and Harddisk. Implemented as Read only.

Table 3-86 ENTITY-MIB Constraints (continued)

MIB Object	Notes
entPhysicalAlias	Not supported for transceiver modules, USB and Harddisk. Implemented only as read-write for the following entPhysicalClass entities: • Chassis • Powersupply • Module
entPhysicalMfgDate	Not implemented.

Note The RP2 module contains Harddisk Container for installing the external Harddisk.

Note The RP2 module contains more sensors than RP1. Hence, the indexing of ENTITY-MIB varies for RP2

Note The RP2 contains 2 physical CPUs, but the CPUs are not monitored separately. The monitoring the CPU utilization is the aggregate result of both the CPUs. Hence, the cpmCPUTotalTable object contains only one entry for RP CPUs.

Note Effective from Cisco IOS Release 15.2(4)S, the entPhysicalIsFRU object for the 6XGE-BUILT-IN SPA in the ASR1002-X chassis is shown as True. This results in the 6XGE-BUILT-IN SPA getting wrongly populated in the cefcModule table.

For the CISCO ASR 1002 Router, RP Module, SIP Module, and SPA Module 0/0 are built-in to the chassis. Table 3-87 lists the values of the affected MIB Objects.

Table 3-87 Affected MIB Objects in CISCO ASR 1002 Router

MIB Object	Module	Value
entPhysicalContainedIn	RP Module	entPhysicalIndex of chassis.
	SIP Module	entPhysicalIndex of chassis.
	SPA Module 0/0	entPhysicalIndex of SIP Module.
entPhysicalIsFRU	RP Module	false(2)
	SIP Module	false(2)
	SPA Module 0/0	false(2)
entPhysicalSerialNum	SPA Module 0/0	No Serial Number
entPhysicalParentRelos	RP Module	0
	ESP Module	0
	SIP Module	0

For the CISCO ASR 1002-F Router, RP Module, SIP Module, SPA Module 0/0, and FP or ESP Module are built-in to the chassis. Table 3-88 lists the values of the affected MIB Objects.

Table 3-88 Affected MIB Objects in Cisco ASR 1002-F Router

MIB Object	Module	Value
entPhysicalContainedIn	RP Module ESP Module SIP Module SPA Module 0/0	entPhysicalIndex of Chassis. entPhysicalIndex of Chassis. entPhysicalIndex of Chassis. entPhysicalIndex of SIP Module.
entPhysicalIsFRU	RP Module ESP Module SIP Module SPA Module 0/0	false(2) false(2) false(2) false(2)
entPhysicalSerialNum	SPA Module 0/0	No Serial Number.
entPhysicalParentRelos	RP Module	0
	ESP Module	0
	SIP Module	0

Note When both primary and secondary RPs are up and running, entities for standby usb flash, Flash disk, and Harddisk are not populated for ENTITY-MIB.

Note For cevModuleASR 1000 UnknownRP object, only RP module entry is populated without any child entities for it.

Note On CEoP SPAs, the entPhysicalFirmware object is mapped to the UFE Field-Programmable Device (FPD).

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 In ASR1002-F, the RP, FP, and SIP support various sensors. These sensors are supported on the CISCO-ENTITY-SENSOR-MIB.

Note Effective from Cisco IOS Release 15.1(3)S, ENTITY-SENSOR-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, the ENTITY-SENSOR-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

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 (Slot container, SPA container, PS bay, and Transceiver Container)
- module (RP, FP, CC, SPA, and Transceiver)
- powerSupply
- fan

Note The ENTITY-STATE-MIB is supported on the Cisco ASR 1001 chassis.

Note Effective from Cisco IOS Release 15.1(3)S, ENTITY-STATE-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

Note Effective from Cisco IOS Release 15.3(1)S, ENTITY-STATE-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

MIB Constraints

Table 3-89 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the ENTITY-STATE-MIB.

Table 3-89 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 associated with either the power supply or the fan.

Note For the RP, FP, CC, and SPA modules, the entStateOper attribute is set to D_entStateOper_enabled if the module is up. Else, the entStateOper attribute is set to D_entStateOper_disabled.

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 3-90 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the ETHER-WIS (RFC 3637) MIB.

Table 3-90 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. Cisco IOS Release 12.2(18)SXF and Cisco IOS Release 12.2(33)SRA support the RFC 2665 version of the MIB. Cisco IOS Release 12.2(33)SRB supports the RFC 3635 version of the MIB.

Note Effective from Cisco IOS Release 15.3(1)S, the ETHERLIKE-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card.

MIB Constraints

Table 3-91 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the ETHERLIKE-MIB. Any objects not listed in a table are implemented as defined in the MIB.

Table 3-91 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.

FRAME-RELAY-DTE-MIB (RFC1315-MIB)

The FRAME-RELAY-DTE-MIB (RFC1315-MIB) contains objects to manage a Frame Relay data terminal equipment (DTE) interface, which consists of a single physical connection to the network with many virtual connections to other destinations and neighbors. The MIB contains the objects used to manage:

- The Data Link Connection Management Interface (DLCMI)
- Virtual circuits on each Frame Relay interface
- Errors detected on Frame Relay interfaces

MIB Constraints

Table 3-92 lists the constraints that the router places on the objects in the RFC1315-MIB.

Table 3-92 FRAME-RELAY-DTE-MIB Constraints

MIB Object	Notes
frDlcmiTable	
• frDlcmiAddress	Always q922November90(3), which indicates a 10-bit DLCI.
• frDlcmiAddressLen	Always two-octets(2).
frCircuitTable	
• frCircuitCommittedBurst • frCircuitExcessBurst • frCircuitThroughput	Normally, the QoS configuration entered through the Modular QoS CLI (MQC) syntax does not appear in these frCircuitTable objects. However, when QoS is configured through the MQC and the following conditions are met, these frCircuitTable objects contain the QoS values as they are entered through the MQC: • The default class is configured on the policy-map only. • An output policy is attached to the Frame Relay (FR) Permanent Virtual Circuit (PVC). • The Cisco class-based-QoS (CBQ) enhancement only supports two MQC actions: police cir and shape. • If both police cir and shape actions exist, then the FR traffic-shaping QoS takes precedence before policing.
frCircuitState	
• frErrTable	Not supported.

HC-ALARM-MIB

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

MIB Tables

Table 3-93 lists the tables in HC-ALARM-MIB.

Table 3-93 HC-ALARM-MIBTables

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

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.

- The IF-MIB supports the Circuit Emulation (CEM) only on the SPA-1CHOC3-CE-ATM. For each controller, only a single CEM interface is supported bacause it is being used for l1/l2 forwarding.
- Multiple sublayers are not supported for the SPA-1CHOC3-CE-ATM from SNMP. Hence, the layers corresponding to digital signal layer 1 (DS1), Synchronous Transport Signal (STS), and Virtual Tributary (VT) are not modeled for the CE interface.

Note Effective from Cisco IOS Release 15.1(3)S, IF-MIB is supported on SPA-24CHT1-CE-ATM and SPA-2CHT3-CE-ATM.

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

Note Effective from Cisco IOS Release 15.3(1)S, the IF-MIB is supported on the Cisco ASR1000: 40G Native Ethernet Line Card and SPA-8XT3/E3.

Note The Cisco ASR1000: 40G Native Ethernet Line Card 2x10GE + 20x1GE supports a total number of 22 ports. Interface numbering is continuous from 0-19 for GE ports and 20-21 for 10GE ports. You can configure interface GigabitEthernet 0/0/x as well as TenGigabitEthernet 0/0/y at the same time, where x = 0 till 19 and y = 20 and 21).

MIB Constraints

Table 3-94 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the IF-MIB.

Table 3-94 IF-MIB Constraints

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

Note To define a Virtual port of a service engine connecting the RP and SE, set the value of ifType to ethernetCsmacd and ifDescr to Service-Engine. The physical port of the SPA is not controlled by the router, the router controls the virtual port of the SPA. This interface is named using in Service-Engine 1/1/0 command and functions as a Gigabit Ethernet Interface. Since, a sub-interface can not be created on this interface, ifStackTable is not implemented.

Note The valueof ifLastChange is always 0 for VT layer in SPA-1xCHSTM1/OC3.

IGMP-STD-MIB (RFC 2933)

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

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.

MIB Constraints

Table 3-95 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the IP-FORWARD-MIB.

Table 3-95 IP-FORWARD-MIB Constraints

MIB Object	Notes
inetCidrRouteTable	Implemented for IPv6 only.

IP-MIB (RFC 4293)

The IP-MIB (RFC 4293) module contains objects for managing IP and Internet Control Message Protocol (ICMP) implementations, but excluding their management of IP routes.

Note The IP-MIB supports both IPv4 and IPv6 networks.

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 3-96 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the IPMROUTE-STD-MIB.

Table 3-96 IPMROUTE-STD-MIB Constraints

MIB Object	Notes
ipMRouteScopeNameTable	Not implemented.
ipMRouteEnable	Read only.
ipMRouteInterfaceTtl	Read only.
ipMRouteInterfaceRateLimit	Read only.

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 (MPLS), Label Distribution Protocol (LDP), 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-MIB

The MPLS-TE-MIB enables the Cisco ASR 1000 Series Routers to perform traffic engineering for MPLS tunnels. The MIB is based on Revision 05 of the IETF MPLS-TE-MIB.

Traffic engineering support for MPLS tunnels requires the following configuration:

- Setting up MPLS tunnels with appropriate configuration parameters.
- Configuring tunnel loose and strict source routed hops.

MIB Constraints

Table 3-97 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the MPLS-TE-MIB.

Table 3-97 MPLS-TE-MIB Constraints

MIB Object	Notes
mplsTunnelIndexNext	Read only. Always 0.
mplsTunnelTable	
• mplsTunnelName	Read only.
• mplsTunnelDescr	Read only.
• mplsTunnelIsif	Read only.
• mplsTunnelXCPointer	Read only.
• mplsTunnelSignallingProto	Read only.
• mplsTunnelSetupPrio	Read only. Always 7.
• mplsTunnelHoldingPrio	Read only. Always 7.
• mplsTunnelSessionAttributes	Read only.
• mplsTunnelOwner	Read only.
• mplsTunnelLocalProtectInUse	Read only. Always false(2).
• mplsTunnelResourcePointer	Read only.
• mplsTunnelInstancePriority	Read only. Always 0.
• mplsTunnelHopTableIndex	Read only.
• mplsTunnelIncludeAnyAffinity	Read only. Always 0.
• mplsTunnelIncludeAllAffinity	Read only.
• mplsTunnelExcludeAllAffinity	Read only.
• mplsTunnelPathInUse	Read only.
• mplsTunnelRole	Read only.

Table 3-97 MPLS-TE-MIB Constraints (continued)

MIB Object	Notes
• mplsTunnelTotalUpTime	Read only.
• mplsTunnelInstanceUpTime	Read only. Always 0.
• mplsTunnelAdminStatus	Read only.
• mplsTunnelRowStatus	Read only. Always readOnly(5).
• mplsTunnelStorageType	Read only. Volatile(2). Always active.
mplsTunnelHopListIndexNext	Read only. Always 0.
mplsTunnelHopTable	
• mplsTunnelHopAddrType	Read only. Always ipv4(1).
• mplsTunnelHopIpv4Addr	Read only.
• mplsTunnelHopIpv4PrefixLen	Read only. Always 32.
• mplsTunnelHopIpv6Addr	Read only. NULL.
• mplsTunnelHopIpv6PrefixLen	Read only. Always 0.
• mplsTunnelHopAsNumber	Read only.
• mplsTunnelHopLspId	Read only.
• mplsTunnelHopType	Read only. Always strict(1).
• mplsTunnelHopRowStatus	Read only. Always active(1).
• mplsTunnelHopStorageType	Read only. Value is readOnly(5).
mplsTunnelResourceIndexNext	Read only. Always 0.
mplsTunnelResourceTable	
• mplsTunnelResourceMaxRate	Read only.
• mplsTunnelResourceMeanRate	Read only.
• mplsTunnelResourceMaxBurstSize	Read only.
• mplsTunnelResourceRowStatus	Read only. Always active(1).

Table 3-97 MPLS-TE-MIB Constraints (continued)

MIB Object	Notes
• mplsTunnelResourceStorageType	Read only. Value is readOnly(5).

Notes:

The mplsTunnelTable allows new MPLS tunnels to be created between an MPLS LSR and a remote endpoint and existing tunnels to be reconfigured or removed. The Cisco ASR 1000 Series Routers support point-to-point tunnel segments, although multipoint-to-point and point-to-multipoint connections are supported by an LSR acting as a cross-connect. Each MPLS tunnel can have one out-segment originating at an LSR and one in-segment terminating at that LSR. The mplsTunnelTable is enhanced by the mplsTunnelPerfTable that provides several counters to measure the performance of the MPLS tunnels.

The mplsTunnelResourceTable indicates the resources required for a tunnel. Multiple tunnels can share the same resources by pointing to the same entry in this table. Tunnels that do not share resources must point to separate entries in this table.

The mplsTunnelHopTable indicates strict or loose hops for an MPLS tunnel defined in mplsTunnelTable when you establish the hop using signaling. Multiple tunnels share the same hops by pointing to the same entry in this table. Each row also has a secondary index, mplsTunnelHopIndex, corresponding to the next hop of this tunnel. The scalar mplsTunnelMaxHops indicates the maximum number of hops that you can specify on each tunnel supported by this LSR. The mplsTunnelARHopTable indicates the actual hops crossed by a tunnel as reported by the MPLS signaling protocol after the tunnel is set up.

There are three notifications in this MIB. The notifications mplsTunnelUp and mplsTunnelDown indicate that the value of mplsTunnelOperStatus has transitioned to up(1) or down(2). The notification mplsTunnelRerouted is generated when a tunnel is rerouted or re-optimized.

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 3-98 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the MPLS-VPN-MIB.

Table 3-98 MPLS-VPN-MIB Constraints

MIB Object	Notes
mplsNumVrfSecViolationThreshExceeded	Not implemented.
mplsVpnVrfSecTable	
• mplsVpnVrfSecIllegalLabelViolations	Read only. Always 0.
• mplsVpnVrfSecIllegalLabelRcvThresh	Read only. Always 0.

Table 3-98 MPLS-VPN-MIB Constraints (continued)

MIB Object	Notes
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.
• 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 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.

Table 3-98 MPLS-VPN-MIB Constraints (continued)

MIB Object	Notes
• 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 3-99 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the NHRP-MIB.

Table 3-99 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.

OLD-CISCO-CHASSIS-MIB

The OLD-CISCO-CHASSIS-MIB describes chassis objects in a device running an old implementation of the Cisco IOS operating system. The chassis objects are now described in the ENTITY-MIB, and OLD-CISCO-CHASSIS-MIB is not supported for Cisco ASR 1000 Series Routers.

OLD-CISCO-SYS-MIB

The OLD-CISCO-SYS-MIB defines objects to manage the system bootstrap description and the corresponding version identification.

Note Currently, only the whyReload object is supported in this MIB.

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 3-100 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the PIM-MIB.

Table 3-100 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.

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 1000 Series Routers.

RSVP-MIB

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

MIB Constraints

Table 3-101 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the RSVP-MIB.

Table 3-101 RSVP-MIB Constraints

MIB Object	Notes
rsvpIfRefreshBlockadeMultiple	Read only.
rsvpIfRefreshMultiple	Read only.

Table 3-101 RSVP-MIB Constraints (continued)

MIB Object	Notes
rsvpIfTTL	Read only.
rsvpIfRefreshInterval	Read only.
rsvpIfRouteDelay	Read only.
rsvpIfUdpRequired	Read only.

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.

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.

Note 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
```

SONET-MIB (RFC 2558)

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

Note The ASR 1000 Series Routers use GR253 standards for SES calculation for path/line/section. Hence, the SNMP query for sonetSESthresholdSet will return ansi1993(3).

Note The SONET-MIB is not supported on SPA-1X10GE-WL-V2 although the SONET alarms listed in Table 3-20 are supported for the Ethernet WIS Port.

MIB Constraints

Table 3-102 lists the constraints that the Cisco ASR 1000 Series Routers place on the objects in the SONET-MIB.

Table 3-102 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.

Table 3-102 SONET-MIB Constraints (continued)

MIB Object	Notes
- sonetMediumLoopbackConfig	Read only.
sonetSESthresholdSet	Read only.

Note When the SONET path is initialized and no active alarms exist, the value of sonetPathCurrentStatus object is zero.

Note If an alarm is triggered and cleared, the value of sonetPathNoDefect object is one.

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.

CHAPTER 4

Monitoring Notifications

This chapter describes the Cisco ASR 1000 Series Aggregation Services Routers notifications supported by the MIB enhancements feature introduced in Cisco IOS Release 12.2(33r)XN. SNMP uses notifications to report events on a managed device. 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, page 4-1
- Enabling Notifications, page 4-2
- Cisco SNMP Notifications, page 4-2

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 1000 Series Routers 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 has changed.	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 field-replaceable unit, such as Cisco ASR 1000 Series Route Processor1 (RP), Cisco ASR 1000 Series Embedded Services Processor (ESP), Cisco ASR 1000 Series SPA Interface Processor (SIP), shared port adapter (SPA) modules, fan, port, power supply, or redundant power supply was added.	No action is required.

Table 4-1 Environmental or Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
cefcFRURemoved	Indicates that a FRU was removed.	A field-replaceable unit, such as RP1, ESP, SIP and SPA modules, fan, ports, power supply, or redundant power supply was removed.	Replace the field-replaceable unit.
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 changes.	When the dsx1LineStatus reports failures, 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.
ciscoSonetSectionStatusChange	Indicates that the value of sonetSectionCurrentStatus has changed.	Section loss of: • Frame failure • Signal failure	Enter the **show controllers** command for the POS interface and check that the Alarm Defects are None and Active Alarms are Zero.
ciscoSonetPathStatusChange	Indicates that the value of sonetPathCurrentStatus has changed.	Caused due to: • sonetPathSTSLOP • sonetPathSTSAIS • sonetPathSTSRDI • sonetPathUnequipped • sonetPathSignalLabelMismatch	Enter the **show controllers** command for the POS interface and check that the Alarm Defects are None and Active Alarms are Zero.

Table 4-2 lists ENTITY-MIB notifications generated by Cisco ASR 1000 Series Routers RPs, ESPs, SPAs and SIP Cards.

Table 4-2 RP, ESPs, SPAs, SIP Card Notifications

Event	Description	Probable Cause	Recommended Action
entConfigChange	An entry for the SIP/SPA/Transceiver module is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change).	A SIP/SPA/Transceiver module was removed.	Replace the field-replaceable unit.
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 RP 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 SPA, then you get the SPA error.	Check the entPhysicalDescr type and take the corresponding action; there are many types of asserted alarms.

Table 4-2 RP, ESPs, SPAs, SIP 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.

When a new alarm condition is detected, the carrier alarm LEDs in the individual line cards are currently set by the line card software. The Cisco IOS alarm subsystem does not control the LEDs.

Starting with Release 3.1, alarm description field is added to the ceAlarmCleared and ceAlarmAsserted event notificaitons.

Flash Device Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco ASR 1000 Series Routers 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 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 RPs are too large to fit in the DF table for one VPN. Try to configure the groups among existing RPs in the hardware, or configure the RP 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 the Border Gateway Protocol (BGP) state changes generated by the Cisco ASR 1000 Series Routers 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.	

Cisco Routing Protocol Notifications

Table 4-8 lists the CISCO-BGP4-MIB notifications that occur during the state changes.

Table 4-8 Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
cbgpFsmStateChange	This notification is generated for every BGP FSM state change.	BGP FSM state change.	
cbgpBackwardTransition	This notification is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	BGP FSM state changes from a higher to a lower numbered state.	This threshold value is configured using the CLI command **neighbor** *nbr_addr max_prefixes* [*threshold*] [*warning-only*].
cbgpPrefixThresholdExceeded	This notification is generated when prefix count exceeds the configured warning threshold on a session for an address family.	The prefix count exceeds the configured warning threshold on a session.	
cbgpPrefixThresholdClear	This notification is generated when prefix count drops below the configured clear threshold on a session for an address family after the cbgpPrefixThresholdExceeded notification is generated.	The prefix count drops below the configured clear threshold on a session.	
cbgpPeer2EstablishedNotification	This notification is generated when the BGP FSM enters the established state.	BGP FSM enters the established state.	
cbgpPeer2BackwardTransNotification	This notification is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	BGP FSM moves from a higher numbered state to a lower numbered state.	
cbgpPeer2FsmStateChange	This notification is generated for every BGP FSM state change.	BGP FSM state change.	
cbgpPeer2BackwardTransition	This notification is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.	BGP FSM moves from a higher numbered state to a lower numbered state.	

Table 4-8 Routing Protocol Notifications (continued)

Event	Description	Probable Cause	Recommended Action
cbgpPeer2PrefixThresholdExceeded	This notification is generated when the prefix count exceeds the configured warning threshold in a session for an address family.	The prefix count exceeds the configured warning threshold in a session for an address family.	
cbgpPeer2PrefixThresholdClear	This notification is generated when the prefix count drops below the configured clear threshold in a session for an address family after the cbgpPeer2PrefixThresholdExceeded notification is generated. This notification is not generated if the peer session goes down after the cbgpPrefixThresholdExceeded notification.	The prefix count drops below the configured clear threshold in a session for an address family.	

RTT Monitor Notifications

Table 4-9 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

Table 4-9 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 4-10 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 4-10 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

Table 4-11 lists CISCO-PROCESS-MIB notifications that can occur.

Table 4-11 CISCO-PROCESS-MIB Notifications

Event	Description	Probable Cause	Recommended Action
cpmCPURisingThreshold	Indicates the rising threshold for system-wide CPU utilization.	When the system-wide CPU utilization crosses (exceeds) the rising threshold, a notification (SNMP/Syslog) is generated. After sending a rising threshold notification, a second rising threshold notification will be sent only if a falling threshold notification corresponding to the first rising threshold notification has been sent.	—
cpmCPUFallingThreshold	Indicates the falling threshold for system-wide CPU utilization.	If the system-wide CPU utilization falls below the falling threshold, a notification is generated. The falling threshold notification is generated only if a rising threshold notification had been sent out previously.	—

QFP Notifications

Table 4-12 lists CISCO-ENTITY-QFP-MIB notifications generated by the Cisco ASR 1000 Series Router.

Table 4-12 CISCO-ENTITY-QFP-MIB Notifications

Event	Description	Probable Cause	Recommended Action
ceqfpMemoryResRisingThreshNotif	Indicates that the QFP memory usage is equal to or greater than the rising threshold limit (ceqfpMemoryResRisingThreshold).	Occurs when the memory usage exceeds the upper threshold limit.	—
ceqfpMemoryResFallingThreshNotif	Indicates that the QFP memory usage is equal to or less than the falling threshold limit(ceqfpMemoryResFallingThreshold).	Occurs when the memory usage falls below the lower threshold limit.	—

Unified Firewall Notifications

Table 4-13 lists CISCO-UNIFIED-FIREWALL-MIB notifications generated by firewall subsystem. ASR 1000 platform only supports the statistics for the zone base firewall in CISCO-UNIFIED-FIREWALL-MIB; notifications listed in Table 4-1 are now supported.

Table 4-13 CISCO-UNIFIED-FIREWALL-MIB Notifications

Event	Description	Probable Cause	Recommended Action
ciscoUFwUrlfServerStateChange	Indicates that the firewall selected a new primary URL filtering server from the existing list of available servers.	Occurs when the current primary server becomes unavailable or when a server is explicitly nominated as primary filtering server.	—
ciscoUFwL2StaticMacAddressMoved	Indicates that the firewall detected change in a static MAC address to a new port.	Occurs when: • The device with the MAC Address is physically moved to a new port. • MAC address is explicitly moved to a new location. • MAC address spoofing is encountered in the system.	—

Image License Management Notifications

Table 4-14 lists the CISCO-IMAGE-LICENSE-MGMT-MIB notifications.

Table 4-14 CISCO-IMAGE-LICENSE-MGMT-MIB Notifications

Event	Description	Probable Cause	Recommended Action
cilmBootImageLevelChanged	Indicates that the boot image level is changed.	Occurs when the boot image level is changed in the management entity.	—

License Management Notifications

Table 4-15 lists the CISCO-LICENSE-MGMT-MIB notifications.

Table 4-15 CISCO-LICENSE-MGMT-MIB Notifications

Event	Description	Probable Cause	Recommended Action
clmgmtLicenseExpired	Indicates that a license has expired.	Occurs when a license expires.	—
clmgmtLicenseExpiryWarning	Indicates that a license is about to expire.	Occurs when a license is about to expire.	—

Table 4-15 CISCO-LICENSE-MGMT-MIB Notifications (continued)

Event	Description	Probable Cause	Recommended Action
clmgmtLicenseUsageCountExceeded	Indicates that the value of the clmgmtLicenseUsage CountRemaining attribute has reached the clmgmtLicenseMaxUsageCount threshold value for a counting license.	Occurs when the value of clmgmtLicenseUsageCountRemaining has reached clmgmtLicenseMaxUsageCount for a counting license.	—
clmgmtLicenseUsageCountAboutToExceed	Indicates that the value of the clmgmtLicenseUsage CountRemaining attribute has reached 80% of the clmgmtLicenseMaxUsageCount for a counting license.	Occurs when clmgmtLicenseUsageCountRemaining has reached 80% of clmgmtLicenseMaxUsageCount for a counting license.	—
clmgmtLicenseInstalled	Indicates that a license is installed successfully.	Occurs when a license is installed successfully.	—
clmgmtLicenseCleared	Indicates that a license is cleared successfully.	Occurs when a license is cleared successfully.	—
clmgmtLicenseRevoked	Indicates that a license is revoked successfully.	Occurs when a license is revoked successfully.	—
clmgmtLicenseEULAAccepted	Indicates that a user has accepted the End-User License Agreement (EULA) for a license.	Occurs when a user accepts the EULA for a license.	—
clmgmtLicenseNotEnforced	Indicates that a license does not exist for a mandatory feature.	Occurs when a license does not exist for a mandatory feature.	—
clmgmtLicenseSubscriptionExpiryWarning	Indicates that the subscription license of a feature is about to expire.	Occurs when the subscription license of a feature is about to expire.	—
clmgmtLicenseSubscriptionExtExpiryWarning	Indicates that the subscription license of a feature has expired but the extension period is available.	Occurs when that the subscription license of a feature has expired but the extension period is available.	—

Table 4-15 CISCO-LICENSE-MGMT-MIB Notifications (continued)

Event	Description	Probable Cause	Recommended Action
clmgmtLicenseSubscriptionExpired	Indicates that the subscription license of a feature has expired.	Occurs when the subscription license of a feature has expired.	—
clmgmtLicenseEvalRTUTransitionWarning	Indicates that an evaluation license is about to be transitioned an a Right -to-Use (RTU) license.	Occurs when evaluation license is about to be transitioned as a RTU license.	—
clmgmtLicenseEvalRTUTransition	Indicates that a feature license has transitioned from an evaluation license to an RTU license.	Occurs when a feature license has transitioned from being an evaluation license to an RTU license.	—

APPENDIX A

Using MIBs

This chapter describes how to perform tasks on the Cisco ASR 1000 Series 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

This section describes

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.

Levels of Redundancy

This section describes the levels of redundancy supported on the Cisco ASR 1000 Series Routers and how to verify that this feature is available. Cisco ASR 1000 Series Routers support fault resistance by allowing a Cisco redundant supervisor engine (SE) to take over if the active supervisor engine 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 processors. One acts as the active route processor while the other acts as the standby route processor.

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

- Cisco IOS software failure
- Cisco ASR 1000 Series Route Processor (RP) hardware failure
- Software upgrade
- Maintenance procedure

Cisco ASR 1000 Series Routers can operate in one of two redundancy modes:

- Route Processor Redundancy (RPR) mode
- Nonstop Forwarding/Stateful Switchover (NSF/SSO) mode

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

Route Processor Redundancy

This section describes the Route Processor Redundancy (RPR) mode for the Cisco ASR 1000 Series Routers.

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

Cisco ASR 1000 Series Routers support fault resistance by allowing a redundant supervisor engine to take over if the active supervisor engine fails.

Cisco Nonstop Forwarding and Stateful Switchover

This section describes the Cisco Nonstop Forwarding and Stateful Switchover mode. With NSF/SSO, Cisco ASR 1000 Series Routers can fail over from the active to the standby route processor almost immediately while continuing to forward packets. Cisco IOS software NSF/SSO support on this platform enables immediate failover.

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

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

Cisco Nonstop Forwarding (NSF) works with the Stateful Switchover (SSO) to minimize the amount of time a network is unavailable to its users following a Route Processor (RP) fail-over in a router with dual RPs. 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.

Cisco NSF works with the Stateful Switchover (SSO) feature in Cisco IOS software to minimize the amount of time a network is unavailable to its users following a switchover. The main objective of Cisco NSF/SSO is to continue forwarding data packets along known routes while the routing protocol information is being restored following a route switchover.

Note For detailed information about the 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

Software Redundancy

Cisco ASR 1004 Routers having only one RP slot do not support hardware redundancy. Instead, these Routers have option of sofware redundancy by running two IOSD processes. IOSD can optionally be run in a redundant configuration. One IOSD instance is active and the other is maintained in a hot standby mode. State information is exchanged between the instances using the normal SSO support over IPC. Software redundancy option is not available and is deactivated if a second RP is added to the chassis. The active RP is responsible for controlling both the active and standby FP as well as all of the I/O (carrier) cards. If the active IOSD instance fails then the backup takes over and resynchronizes its state with the FP and I/O cards.

Verifying Cisco ASR 1000 Series Routers Redundancy

To display information about the active and standby supervisor engines installed in a Cisco ASR 1000 Series Routers, use the **show redundancy** command and **show redundancy states** command. For Router Processor 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 Router Processor in R1 slot.

Example A-1 Displaying Redundancy States from Active Processor

```
R5-mcp-6ru-2#sh redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
        Unit ID = 48

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

   client count = 66
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

R5-mcp-6ru-2#exit
```

Example A-2 Displaying Redundancy States from Standby Processor

```
R5-mcp-6ru-2-stby#sh redundancy state
       my state = 8  -STANDBY HOT
     peer state = 13 -ACTIVE
           Mode = Duplex
        Unit ID = 49

Redundancy Mode (Operational) = sso
Redundancy Mode (Configured)  = sso
Redundancy State              = sso
```

```
     Maintenance Mode = Disabled
    Manual Swact = cannot be initiated from this the standby unit  Communications = Up

   client count = 67
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

R5-mcp-6ru-2-stby#
```

Example A-3 Displaying Redundancy States for Software Redundancy - ASR 1004

```
R5-mcp-4ru-1#sh redundancy states
       my state = 13 -ACTIVE
     peer state = 8  -STANDBY HOT
           Mode = Duplex
        Unit ID = 48

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

   client count = 66
 client_notification_TMR = 30000 milliseconds
           RF debug mask = 0x0

R5-mcp-4ru-1#
```

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 aboutthe 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
  - Determining the ifIndex Value for a Physical Port, page A-12
  - Monitoring and Configuring FRU Status, page A-12
- Generating SNMP Notifications, page A-23

Purpose and Benefits

The physical entity management feature of the Cisco ASR 1000 Series Routers 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.

Sample of ENTITY-MIB entPhysicalTable Entries

The samples in this section show how information is stored in the entPhysicalTable. You can perform asset inventory by examining entPhysicalTable entries.

Note The sample outputs and values that appear throughout this chapter are examples of data you can view when using MIBs.

The following display shows the ENTITY-MIB entPhysicalTable sample entries for a ASR1000 SIP-10 card installed in a router chassis and four SPAs inserted into the card.

ENTITY-MIB entPhysicalTable Entries

```
entPhysicalDescr.1000 = Cisco ASR1000 SPA Interface Processor 10
entPhysicalDescr.1001 = V1: VMA
entPhysicalDescr.1002 = V1: VMB
entPhysicalDescr.1003 = V1: VMC
entPhysicalDescr.1004 = V1: VMD
entPhysicalDescr.1005 = V1: VME
entPhysicalDescr.1006 = V1: VMF
entPhysicalDescr.1007 = V1: 12v
entPhysicalDescr.1008 = V1: VDD
entPhysicalDescr.1009 = V1: GP1
entPhysicalDescr.1010 = V1: GP2
entPhysicalDescr.1011 = V2: VMB
entPhysicalDescr.1012 = V2: 12v
entPhysicalDescr.1013 = V2: VDD
entPhysicalDescr.1014 = V2: GP2
entPhysicalDescr.1015 = Temp: Left
entPhysicalDescr.1016 = Temp: Center
entPhysicalDescr.1017 = Temp: Asic1
entPhysicalDescr.1018 = Temp: Right
entPhysicalDescr.1026 = CPU 0 of module 0
entPhysicalDescr.1027 = SPA Bay
entPhysicalDescr.1028 = SPA Bay
entPhysicalDescr.1029 = SPA Bay
entPhysicalDescr.1030 = SPA Bay
.....
entPhysicalVendorType.1000 = cevModuleASR1000SIP10
entPhysicalVendorType.1001 = cevSensor
entPhysicalVendorType.1002 = cevSensor
entPhysicalVendorType.1003 = cevSensor
entPhysicalVendorType.1004 = cevSensor
entPhysicalVendorType.1005 = cevSensor
entPhysicalVendorType.1006 = cevSensor
entPhysicalVendorType.1007 = cevSensor
entPhysicalVendorType.1008 = cevSensor
entPhysicalVendorType.1009 = cevSensor
entPhysicalVendorType.1010 = cevSensor
entPhysicalVendorType.1011 = cevSensor
entPhysicalVendorType.1012 = cevSensor
entPhysicalVendorType.1013 = cevSensor
entPhysicalVendorType.1014 = cevSensor
entPhysicalVendorType.1015 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1016 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1017 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1018 = cevSensorModuleDeviceTemp
entPhysicalVendorType.1026 = cevModuleCpuType
entPhysicalVendorType.1027 = cevContainerSPABay
entPhysicalVendorType.1028 = cevContainerSPABay
entPhysicalVendorType.1029 = cevContainerSPABay
entPhysicalVendorType.1030 = cevContainerSPABay
....
```

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

```
entPhysicalContainedIn.1000 = 2
entPhysicalContainedIn.1001 = 1000
entPhysicalContainedIn.1002 = 1000
entPhysicalContainedIn.1003 = 1000
entPhysicalContainedIn.1004 = 1000
entPhysicalContainedIn.1005 = 1000
entPhysicalContainedIn.1006 = 1000
entPhysicalContainedIn.1007 = 1000
entPhysicalContainedIn.1008 = 1000
entPhysicalContainedIn.1009 = 1000
entPhysicalContainedIn.1010 = 1000
entPhysicalContainedIn.1011 = 1000
entPhysicalContainedIn.1012 = 1000
entPhysicalContainedIn.1013 = 1000
entPhysicalContainedIn.1014 = 1000
entPhysicalContainedIn.1015 = 1000
entPhysicalContainedIn.1016 = 1000
entPhysicalContainedIn.1017 = 1000
entPhysicalContainedIn.1018 = 1000
entPhysicalContainedIn.1026 = 1000
entPhysicalContainedIn.1027 = 1000
entPhysicalContainedIn.1028 = 1000
entPhysicalContainedIn.1029 = 1000
entPhysicalContainedIn.1030 = 1000
```

where **entPhysicalContainedIn** indicates the entPhysicalIndex of a component’s parent entity.

```
entPhysicalClass.1000 = module(9)
entPhysicalClass.1001 = sensor(8)
entPhysicalClass.1002 = sensor(8)
entPhysicalClass.1003 = sensor(8)
entPhysicalClass.1004 = sensor(8)
entPhysicalClass.1005 = sensor(8)
entPhysicalClass.1006 = sensor(8)
entPhysicalClass.1007 = sensor(8)
entPhysicalClass.1008 = sensor(8)
entPhysicalClass.1009 = sensor(8)
entPhysicalClass.1010 = sensor(8)
entPhysicalClass.1011 = sensor(8)
entPhysicalClass.1012 = sensor(8)
entPhysicalClass.1013 = sensor(8)
entPhysicalClass.1014 = sensor(8)
entPhysicalClass.1015 = sensor(8)
entPhysicalClass.1016 = sensor(8)
entPhysicalClass.1017 = sensor(8)
entPhysicalClass.1018 = sensor(8)
entPhysicalClass.1026 = other(1)
entPhysicalClass.1027 = container(5)
entPhysicalClass.1028 = container(5)
entPhysicalClass.1029 = container(5)
entPhysicalClass.1030 = container(5)
```

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

```
entPhysicalParentRelPos.1000 = 0
entPhysicalParentRelPos.1001 = 0
entPhysicalParentRelPos.1002 = 1
entPhysicalParentRelPos.1003 = 2
entPhysicalParentRelPos.1004 = 3
entPhysicalParentRelPos.1005 = 4
entPhysicalParentRelPos.1006 = 5
entPhysicalParentRelPos.1007 = 6
entPhysicalParentRelPos.1008 = 7
entPhysicalParentRelPos.1009 = 8
entPhysicalParentRelPos.1010 = 9
entPhysicalParentRelPos.1011 = 10
entPhysicalParentRelPos.1012 = 11
entPhysicalParentRelPos.1013 = 12
entPhysicalParentRelPos.1014 = 13
entPhysicalParentRelPos.1015 = 14
entPhysicalParentRelPos.1016 = 15
entPhysicalParentRelPos.1017 = 16
entPhysicalParentRelPos.1018 = 17
entPhysicalParentRelPos.1026 = 0
entPhysicalParentRelPos.1027 = 0
entPhysicalParentRelPos.1028 = 1
entPhysicalParentRelPos.1029 = 2
entPhysicalParentRelPos.1030 = 3
```

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

```
entPhysicalName.1000 = module 0
entPhysicalName.1001 = V1: VMA 0/0
entPhysicalName.1002 = V1: VMB 0/1
entPhysicalName.1003 = V1: VMC 0/2
entPhysicalName.1004 = V1: VMD 0/3
entPhysicalName.1005 = V1: VME 0/4
entPhysicalName.1006 = V1: VMF 0/5
entPhysicalName.1007 = V1: 12v 0/6
entPhysicalName.1008 = V1: VDD 0/7
entPhysicalName.1009 = V1: GP1 0/8
entPhysicalName.1010 = V1: GP2 0/9
entPhysicalName.1011 = V2: VMB 0/10
entPhysicalName.1012 = V2: 12v 0/11
entPhysicalName.1013 = V2: VDD 0/12
entPhysicalName.1014 = V2: GP2 0/13
entPhysicalName.1015 = Temp: Left 0/14
entPhysicalName.1016 = Temp: Center 0/15
entPhysicalName.1017 = Temp: Asic1 0/16
entPhysicalName.1018 = Temp: Right 0/17
entPhysicalName.1026 = cpu 0/0
entPhysicalName.1027 = subslot 0/0
entPhysicalName.1028 = subslot 0/1
entPhysicalName.1029 = subslot 0/2
entPhysicalName.1030 = subslot 0/3
```

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

```
entPhysicalHardwareRev.1000 = V00
entPhysicalHardwareRev.1001 =
entPhysicalHardwareRev.1002 =
entPhysicalHardwareRev.1003 =
entPhysicalHardwareRev.1004 =
entPhysicalHardwareRev.1005 =
entPhysicalHardwareRev.1006 =
entPhysicalHardwareRev.1007 =
entPhysicalHardwareRev.1008 =
entPhysicalHardwareRev.1009 =
entPhysicalHardwareRev.1010 =
entPhysicalHardwareRev.1011 =
entPhysicalHardwareRev.1012 =
entPhysicalHardwareRev.1013 =
entPhysicalHardwareRev.1014 =
entPhysicalHardwareRev.1015 =
entPhysicalHardwareRev.1016 =
entPhysicalHardwareRev.1017 =
entPhysicalHardwareRev.1018 =
entPhysicalHardwareRev.1026 =
entPhysicalHardwareRev.1027 =
entPhysicalHardwareRev.1028 =
entPhysicalHardwareRev.1029 =
entPhysicalHardwareRev.1030 =
```

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

```
entPhysicalSerialNum.1000 = JAB11090506
entPhysicalSerialNum.1001 =
entPhysicalSerialNum.1002 =
entPhysicalSerialNum.1003 =
entPhysicalSerialNum.1004 =
entPhysicalSerialNum.1005 =
entPhysicalSerialNum.1006 =
entPhysicalSerialNum.1007 =
entPhysicalSerialNum.1008 =
entPhysicalSerialNum.1009 =
entPhysicalSerialNum.1010 =
entPhysicalSerialNum.1011 =
entPhysicalSerialNum.1012 =
entPhysicalSerialNum.1013 =
entPhysicalSerialNum.1014 =
entPhysicalSerialNum.1015 =
entPhysicalSerialNum.1016 =
entPhysicalSerialNum.1017 =
entPhysicalSerialNum.1018 =
entPhysicalSerialNum.1026 =
entPhysicalSerialNum.1027 =
entPhysicalSerialNum.1028 =
entPhysicalSerialNum.1029 =
entPhysicalSerialNum.1030 =
```

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

```
entPhysicalMfgName.1000 = Cisco Systems Inc
entPhysicalMfgName.1001 =
entPhysicalMfgName.1002 =
entPhysicalMfgName.1003 =
entPhysicalMfgName.1004 =
entPhysicalMfgName.1005 =
entPhysicalMfgName.1006 =
entPhysicalMfgName.1007 =
entPhysicalMfgName.1008 =
entPhysicalMfgName.1009 =
entPhysicalMfgName.1010 =
entPhysicalMfgName.1011 =
entPhysicalMfgName.1012 =
entPhysicalMfgName.1013 =
entPhysicalMfgName.1014 =
entPhysicalMfgName.1015 =
entPhysicalMfgName.1016 =
entPhysicalMfgName.1017 =
entPhysicalMfgName.1018 =
entPhysicalMfgName.1026 =
entPhysicalMfgName.1027 =
entPhysicalMfgName.1028 =
entPhysicalMfgName.1029 =
entPhysicalMfgName.1030 =
```

where **entPhysicalMfgName** provides the manufacturer’s name for the physical component.

```
entPhysicalModelName.1000 = ASR1000-SIP10
entPhysicalModelName.1001 =
entPhysicalModelName.1002 =
entPhysicalModelName.1003 =
entPhysicalModelName.1004 =
entPhysicalModelName.1005 =
entPhysicalModelName.1006 =
entPhysicalModelName.1007 =
entPhysicalModelName.1008 =
entPhysicalModelName.1009 =
entPhysicalModelName.1010 =
entPhysicalModelName.1011 =
entPhysicalModelName.1012 =
entPhysicalModelName.1013 =
entPhysicalModelName.1014 =
entPhysicalModelName.1015 =
entPhysicalModelName.1016 =
entPhysicalModelName.1017 =
entPhysicalModelName.1018 =
entPhysicalModelName.1026 =
entPhysicalModelName.1027 =
entPhysicalModelName.1028 =
entPhysicalModelName.1029 =
entPhysicalModelName.1030 =
```

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

```
entPhysicalIsFRU.1000 = true(1)
entPhysicalIsFRU.1001 = false(2)
entPhysicalIsFRU.1002 = false(2)
entPhysicalIsFRU.1003 = false(2)
entPhysicalIsFRU.1004 = false(2)
entPhysicalIsFRU.1005 = false(2)
entPhysicalIsFRU.1006 = false(2)
entPhysicalIsFRU.1007 = false(2)
entPhysicalIsFRU.1008 = false(2)
entPhysicalIsFRU.1009 = false(2)
entPhysicalIsFRU.1010 = false(2)
entPhysicalIsFRU.1011 = false(2)
entPhysicalIsFRU.1012 = false(2)
entPhysicalIsFRU.1013 = false(2)
entPhysicalIsFRU.1014 = false(2)
entPhysicalIsFRU.1015 = false(2)
entPhysicalIsFRU.1016 = false(2)
entPhysicalIsFRU.1017 = false(2)
entPhysicalIsFRU.1018 = false(2)
entPhysicalIsFRU.1026 = false(2)
entPhysicalIsFRU.1027 = false(2)
entPhysicalIsFRU.1028 = false(2)
entPhysicalIsFRU.1029 = false(2)
entPhysicalIsFRU.1030 = false(2)
```

where **entPhysicalIsFRU** indicates whether or not this physical entity is considered a field replaceable unit (FRU).

Note the following about the sample configuration:

- All chassis slots and line card ports have the same entPhysicalContainedIn value:
  - For chassis slots, entPhysicalContainedIn = 1 (the entPhysicalIndex of the chassis).
  - For SPA ports, the entPhysicalContainedIn = 1280 (the entPhysicalIndex of the SPA card).
- Each chassis slot and line 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
```

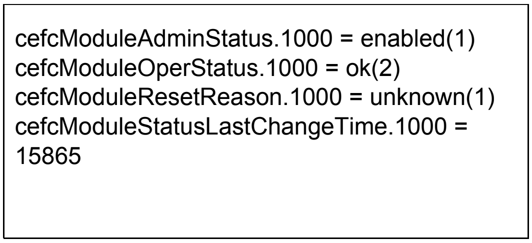
Monitoring and Configuring FRU Status

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 SIP 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-24 for information about how the router generates notifications to indicate changes in FRU status.

Using ENTITY-ALARM-MIB to Monitor Entity Alarms

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 ASR1002 AC power supply in power supply bay 0:

```
ptolemy-265->getmany -v2c 9.0.0.56 public entityMIB | grep "\.4 "
entPhysicalDescr.4 = Cisco ASR1002 AC Power Supply
entPhysicalVendorType.4 = cevPowerSupplyASR1002AC
entPhysicalContainedIn.4 = 3
entPhysicalClass.4 = powerSupply(6)
entPhysicalParentRelPos.4 = 0
entPhysicalName.4 = Power Supply Module 0
entPhysicalHardwareRev.4 = V01
entPhysicalFirmwareRev.4 =
entPhysicalSoftwareRev.4 =
entPhysicalSerialNum.4 = ART1132U00C
entPhysicalMfgName.4 =
entPhysicalModelName.4 = ASR1002-PWR-AC
entPhysicalAlias.4 =
entPhysicalAssetID.4 =
entPhysicalIsFRU.4 = true(1)
entPhysicalMfgDate.4 = 00 00  00 00   00 00  00 00
entPhysicalUris.4 = URN:CLEI:COUPACJBAA
entPhysicalChildIndex.3.4 = 4
```

For more information on this MIB, refer to ENTITY-MIB (RFC 4133), page 3-99.

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 3-31.

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 are the sample output:

```
ptolemy-218->getmany -v2c 9.0.0.56 public ceAlarmDescrMapTable
ceAlarmDescrVendorType.1 = cevPortCT3
ceAlarmDescrVendorType.2 = cevPortT1E1
ceAlarmDescrVendorType.3 = cevPortT3E3
ceAlarmDescrVendorType.4 = cevContainerSFP
ceAlarmDescrVendorType.5 = cevContainerASR1000RPSlot
ceAlarmDescrVendorType.6 = cevContainerASR1000FPSlot
ceAlarmDescrVendorType.7 = cevContainerASR1000CCSlot
ceAlarmDescrVendorType.8 = cevContainerASR1000PowerSupplyBay
ceAlarmDescrVendorType.9 = cevSensorModuleDeviceTemp
ceAlarmDescrVendorType.10 = cevSensorModuleDeviceVoltage
ceAlarmDescrVendorType.11 = cevSensorModuleDeviceCurrent
ceAlarmDescrVendorType.12 = cevSensor
ceAlarmDescrVendorType.13 = cevModuleASR1002RP1
ceAlarmDescrVendorType.14 = cevPortUSB
ceAlarmDescrVendorType.15 = cevPortGe
ceAlarmDescrVendorType.16 = cevModuleASR1000ESP10
ceAlarmDescrVendorType.17 = cevModuleASR1002SIP10
ceAlarmDescrVendorType.18 = cevContainerSPABay
ceAlarmDescrVendorType.19 = cevPowerSupplyASR1002AC
ceAlarmDescrVendorType.20 = cevModuleASR1002Spa4pGe
```

The temperature sensor in ASR1000 modules (RP, FP, CC, and PEM) contains cevSensorModuleDeviceTemp as entPhysicalvendorType OID. From the above sample output, the index (ceAlarmDescrIndex) 9 is mapped to cevSensorModuleDeviceTemp, and the index 19 is mapped to the AER10002 power supply which has cevPowerSupplyASR1002AC as entity physical vendor type OID.

Note SPA is not included in ALL ASR1000 modules. It has its own vendor type OID defined for its sensor.

Note The generic vendor OID, cevSenor, is used in case the ASR1000 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 type of entity in the ASR1000 modules. The index 9 is obtained from the ceAlarmDescrMapTable in the previous section:

```
ptolemy-225->getmany -v2c 9.0.0.56 public 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 Temperature Sensor
ceAlarmDescrText.9.1 = Temp Above Normal (Shutdown)
ceAlarmDescrText.9.2 = Temp Above Normal
ceAlarmDescrText.9.3 = Temp Above Normal
ceAlarmDescrText.9.4 = Temp Above Normal
ceAlarmDescrText.9.5 = Temp Below Normal (Shutdown)
ceAlarmDescrText.9.6 = Temp Below Normal
ceAlarmDescrText.9.7 = Temp Below Normal
ceAlarmDescrText.9.8 = Temp 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 0 is for faulty 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 ASR1002 AC power supply which has cevPowerSupplyASR1002AC as vendor type OID and is mapped to the ceAlarmDescrIndex 19.

```
ptolemy-237->getmany -v2c 9.0.0.56 public ceAlarmDescrTable | grep "\.19\."
ceAlarmDescrSeverity.19.0 = 1
ceAlarmDescrSeverity.19.1 = 1
ceAlarmDescrSeverity.19.2 = 1
ceAlarmDescrSeverity.19.3 = 2
ceAlarmDescrSeverity.19.4 = 2
ceAlarmDescrSeverity.19.5 = 2
ceAlarmDescrText.19.0 = Power Supply Failure
ceAlarmDescrText.19.1 = All Fans Failed
ceAlarmDescrText.19.2 = Multiple Fan Failures
ceAlarmDescrText.19.3 = Fan 0 Failure
ceAlarmDescrText.19.4 = Fan 1 Failure
ceAlarmDescrText.19.5 = Fan 2 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

octet 32:

```
    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
```

From the entity physical table (entPhysicalTable in ENTITY-MIB), we understnd that the ASR1002 AC power supply in power supply bay 0 has 4 as entPhysicalIndex .

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

```
ptolemy-248->getone -v2c 9.0.0.56 public ceAlarmList.4
ceAlarmList.4 =
09 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 ASR1002 AC power supply in the bay 0 has the following alarms asserted:

Alarm type 0 : Power Supply Failure

Alarm type 3 : Fan 0 Failure

As for the ASR1002 AC power supply in bay 1, which has 14 as entPhysiclIndex:

```
ptolemy-247->getone -v2c 9.0.0.56 public ceAlarmList.14
```

ceAlarmList.14 =

Because the length of alarm list returned for the power supply in bay 1 is 0, there is no alarm asserted for the power supply in bay 1.

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

```
R5-mcp-2ru-1#sh facility-alarm status
System Totals  Critical: 2  Major: 1  Minor: 0
Source               Severity      Description [Index]
```

```
------              ---------     -------------------
Cisco ASR1002 AC Power Sup CRITICAL      Power Supply Failure [0]
Cisco ASR1002 AC Power Sup MAJOR         Fan 0 Failure [3]
xcvr container 0/0/1       INFO          Transceiver Missing [0]
xcvr container 0/0/2       CRITICAL      Transceiver Missing - Link Down [1]
xcvr container 0/0/3       INFO          Transceiver Missing [0]
```

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-4 Displaying Sample Output for the Alarm History

```
ptolemy-257->getnext -v2c 9.0.0.56 public ceAlarmHistory
ceAlarmHistTableSize.0 = 200  →  the size of alarm history table
ptolemy-258->getnext -v2c 9.0.0.56 public ceAlarmHistTableSize.0
ceAlarmHistLastIndex.0 = 21  →  the index for the last alarm added
```

Example A-5 Displaying the Last Alarm Action (asserted or cleared) Added to the Alarm History Table

```
ptolemy-259->getmany -v2c 9.0.0.56 public ceAlarmHistTable | grep "\.21 "
ceAlarmHistType.21 = cleared(2)  →  alarm cleared
ceAlarmHistEntPhysicalIndex.21=4  →  it is for physical entity indexed by 4
ceAlarmHistAlarmType.21 = 3  →  alarm type is 3
ceAlarmHistSeverity.21 = major(2)  →  the alarm severity is major(2)
ceAlarmHistTimeStamp.21 = 7506193
```

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-6 Displaying the Physical Entity That has Value 4 as entPhysicalIndex

```
entPhysicalDescr.4 = Cisco ASR1002 AC Power Supply
entPhysicalVendorType.4 = cevPowerSupplyASR1002AC
entPhysicalContainedIn.4 = 3
entPhysicalClass.4 = powerSupply(6)
entPhysicalParentRelPos.4 = 0
entPhysicalName.4 = Power Supply Module 0
entPhysicalHardwareRev.4 = V01
entPhysicalFirmwareRev.4 =
entPhysicalSoftwareRev.4 =
entPhysicalSerialNum.4 = ART1132U00C
entPhysicalMfgName.4 =
entPhysicalModelName.4 = ASR1002-PWR-AC
```

Example A-7 Displaying the Alarm Type Defined for cevPowerSupplyASR1002AC

```
ceAlarmDescrSeverity.19.0 = 1
ceAlarmDescrSeverity.19.1 = 1
ceAlarmDescrSeverity.19.2 = 1
ceAlarmDescrSeverity.19.3 = 2
ceAlarmDescrSeverity.19.4 = 2
ceAlarmDescrSeverity.19.5 = 2
ceAlarmDescrText.19.0 = Power Supply Failure
ceAlarmDescrText.19.1 = All Fans Failed
ceAlarmDescrText.19.2 = Multiple Fan Failures
ceAlarmDescrText.19.3 = Fan 0 Failure
ceAlarmDescrText.19.4 = Fan 1 Failure
ceAlarmDescrText.19.5 = Fan 2 Failure
```

From the alarm type defined for cevPowerSupplyASR1002AC, the application can easily interpret the last entry in the alarm history table as : Fan 0 Failure Alarm is Cleared for Cisco ASR1002 AC Power Supply in power supply bay 0.

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-8 Displaying the Sample Notification Received

```
Received SNMPv2c Trap:
Community: public
From: 9.0.0.56
sysUpTimeInstance = 7500792
snmpTrapOID.0 = ceAlarmCleared
ceAlarmHistEntPhysicalIndex.19 = 4
ceAlarmHistAlarmType.19 = 0
ceAlarmHistSeverity.19 = critical(1)
ceAlarmHistTimeStamp.19 = 7500792


Received SNMPv2c Trap:
Community: public
From: 9.0.0.56
sysUpTimeInstance = 7504592
snmpTrapOID.0 = ceAlarmAsserted
ceAlarmHistEntPhysicalIndex.20 = 4
ceAlarmHistAlarmType.20 = 3
ceAlarmHistSeverity.20 = major(2)
ceAlarmHistTimeStamp.20 = 7504592


Received SNMPv2c Trap:
Community: public
From: 9.0.0.56
sysUpTimeInstance = 7506193
snmpTrapOID.0 = ceAlarmCleared
ceAlarmHistEntPhysicalIndex.21 = 4
ceAlarmHistAlarmType.21 = 3
ceAlarmHistSeverity.21 = major(2)
ceAlarmHistTimeStamp.21 = 7506193
```

Entity Containment Tree

The following is sample entity hierarchy for a ASR1002 device, Mib Variables printed : <entPhysicalName entPhysicalClass>

```
ENTITY-MIB containment tree:
    |
    \-1 (cevChassisASR1002) : Chassis : chassis
         |
         +-2 (cevContainerASR1000FPSlot) : slot F0 : container
         |    |
         |    \-9000 (cevModuleASR1000ESP10) : module F0 : module
         |         |
         |         +-9001 (cevSensorModuleDeviceVoltage) : V1: VMA F0/0 : sensor
         |         |
         |         +-9002 (cevSensorModuleDeviceVoltage) : V1: VMB F0/1 : sensor
         |         |
         |         +-9003 (cevSensorModuleDeviceVoltage) : V1: VMC F0/2 : sensor
         |         |
         |         +-9004 (cevSensorModuleDeviceVoltage) : V1: VMD F0/3 : sensor
         |         |
         |         +-9005 (cevSensorModuleDeviceVoltage) : V1: VME F0/4 : sensor
         |         |
         |         +-9006 (cevSensorModuleDeviceVoltage) : V1: 12v F0/5 : sensor
         |         |
         |         +-9007 (cevSensorModuleDeviceVoltage) : V1: VDD F0/6 : sensor
         |         |
         |         +-9008 (cevSensorModuleDeviceVoltage) : V1: GP1 F0/7 : sensor
         |         |
         |         +-9009 (cevSensorModuleDeviceVoltage) : V2: VMA F0/8 : sensor
         |         |
         |         +-9010 (cevSensorModuleDeviceVoltage) : V2: VMB F0/9 : sensor
         |         |
         |         +-9011 (cevSensorModuleDeviceVoltage) : V2: VMC F0/10 : sensor
         |         |
         |         +-9012 (cevSensorModuleDeviceVoltage) : V2: VMD F0/11 : sensor
         |         |
         |         +-9013 (cevSensorModuleDeviceVoltage) : V2: VME F0/12 : sensor
         |         |
         |         +-9014 (cevSensorModuleDeviceVoltage) : V2: VMF F0/13 : sensor
         |         |
         |         +-9015 (cevSensorModuleDeviceVoltage) : V2: 12v F0/14 : sensor
         |         |
         |         +-9016 (cevSensorModuleDeviceVoltage) : V2: VDD F0/15 : sensor
         |         |
         |         +-9017 (cevSensorModuleDeviceVoltage) : V2: GP1 F0/16 : sensor
         |         |
         |         +-9018 (cevSensorModuleDeviceTemp) : Temp: Inlet F0/17 : sensor
         |         |
         |         +-9019 (cevSensorModuleDeviceTemp) : Temp: Asic1 F0/18 : sensor
         |         |
         |         +-9020 (cevSensorModuleDeviceTemp) : Temp: Exhaust1 F0/19 : sensor
         |         |
         |         +-9021 (cevSensorModuleDeviceTemp) : Temp: Exhaust2 F0/20 : sensor
         |         |
         |         \-9022 (cevSensorModuleDeviceTemp) : Temp: Asic2 F0/21 : sensor
         |
         +-3 (cevContainerASR1000PowerSupplyBay) : Power Supply Bay 0 : container
         |    |
         |    \-4 (cevPowerSupplyASR1002AC) : Power Supply Module 0 : powerSupply
         |         |
         |         +-5 (cevSensorModuleDeviceCurrent) : PEM Iout P0/0 : sensor
         |         |
         |         +-6 (cevSensorModuleDeviceVoltage) : PEM Vout P0/1 : sensor
         |         |
         |         +-7 (cevSensorModuleDeviceVoltage) : PEM Vin P0/2 : sensor
         |         |
         |         +-8 (cevSensorModuleDeviceTemp) : Temp: PEM P0/3 : sensor
         |         |
         |         \-9 (cevSensorModuleDeviceTemp) : Temp: FC  P0/4 : sensor
         |
         +-13 (cevContainerASR1000PowerSupplyBay) : Power Supply Bay 1 : container
         |    |
         |    \-14 (cevPowerSupplyASR1002AC) : Power Supply Module 1 : powerSupply
         |         |
         |         +-15 (cevSensorModuleDeviceCurrent) : PEM Iout P1/0 : sensor
         |         |
         |         +-16 (cevSensorModuleDeviceVoltage) : PEM Vout P1/1 : sensor
         |         |
         |         +-17 (cevSensorModuleDeviceVoltage) : PEM Vin P1/2 : sensor
         |         |
         |         +-18 (cevSensorModuleDeviceTemp) : Temp: PEM P1/3 : sensor
         |         |
         |         \-19 (cevSensorModuleDeviceTemp) : Temp: FC  P1/4 : sensor
         |
         +-1000 (cevModuleASR1002SIP10) : module 0 : module
         |    |
         |    +-1001 (cevSensorModuleDeviceVoltage) : V1: VMA 0/0 : sensor
         |    |
         |    +-1002 (cevSensorModuleDeviceVoltage) : V1: VMB 0/1 : sensor
         |    |
         |    +-1003 (cevSensorModuleDeviceVoltage) : V1: VMC 0/2 : sensor
         |    |
         |    +-1004 (cevSensorModuleDeviceVoltage) : V1: VMD 0/3 : sensor
         |    |
         |    +-1005 (cevSensorModuleDeviceVoltage) : V1: VME 0/4 : sensor
         |    |
         |    +-1006 (cevSensorModuleDeviceVoltage) : V1: VMF 0/5 : sensor
         |    |
         |    +-1007 (cevSensorModuleDeviceVoltage) : V1: 12v 0/6 : sensor
         |    |
         |    +-1008 (cevSensorModuleDeviceVoltage) : V1: VDD 0/7 : sensor
         |    |
         |    +-1009 (cevSensorModuleDeviceVoltage) : V1: GP1 0/8 : sensor
         |    |
         |    +-1010 (cevSensorModuleDeviceVoltage) : V1: GP2 0/9 : sensor
         |    |
         |    +-1011 (cevSensorModuleDeviceVoltage) : V2: VMB 0/10 : sensor
         |    |
         |    +-1012 (cevSensorModuleDeviceVoltage) : V2: 12v 0/11 : sensor
         |    |
         |    +-1013 (cevSensorModuleDeviceVoltage) : V2: VDD 0/12 : sensor
         |    |
         |    +-1014 (cevSensorModuleDeviceVoltage) : V2: GP2 0/13 : sensor
         |    |
         |    +-1015 (cevSensorModuleDeviceTemp) : Temp: Left 0/14 : sensor
         |    |
         |    +-1016 (cevSensorModuleDeviceTemp) : Temp: Center 0/15 : sensor
         |    |
         |    +-1017 (cevSensorModuleDeviceTemp) : Temp: Asic1 0/16 : sensor
         |    |
         |    +-1018 (cevSensorModuleDeviceTemp) : Temp: Right 0/17 : sensor
         |    |
         |    +-1026 (cevModuleCpuType) : cpu 0/0 : other
         |    |
         |    +-1027 (cevContainerSPABay) : subslot 0/1 : container
         |    |
         |    +-1028 (cevContainerSPABay) : subslot 0/2 : container
         |    |
         |    +-1029 (cevContainerSPABay) : subslot 0/3 : container
         |    |
         |    \-1040 (cevModuleASR1002Spa4pGe) : SPA subslot 0/0 : module
         |         |
         |         +-1066 (cevSensorModuleDeviceTemp) : subslot 0/0 temperature Sensor 0
         |         |
         |         +-1067 (cevSensorModuleDeviceTemp) : subslot 0/0 temperature Sensor 1
         |         |
         |         +-1091 (cevContainerSFP) : subslot 0/0 transceiver container 0 : cont+
         |         |    |
         |         |    \-1092 (cevSFP1000BaseT) : subslot 0/0 transceiver 0 : module
         |         |         |
         |         |         \-1093 (cevPortGe) : GigabitEthernet0/0/0 : port
         |         |
         |         +-1103 (cevContainerSFP) : subslot 0/0 transceiver container 1 : cont+
         |         |
         |         +-1115 (cevContainerSFP) : subslot 0/0 transceiver container 2 : cont+
         |         |
         |         \-1127 (cevContainerSFP) : subslot 0/0 transceiver container 3 : cont+
         |
         \-7000 (cevModuleASR1002RP1) : module R0 : module
              |
              +-7001 (cevSensorModuleDeviceVoltage) : V1: VMA R0/0 : sensor
              |
              +-7002 (cevSensorModuleDeviceVoltage) : V1: VMB R0/1 : sensor
              |
              +-7003 (cevSensorModuleDeviceVoltage) : V1: VMC R0/2 : sensor
              |
              +-7004 (cevSensorModuleDeviceVoltage) : V1: VMD R0/3 : sensor
              |
              +-7005 (cevSensorModuleDeviceVoltage) : V1: VME R0/4 : sensor
              |
              +-7006 (cevSensorModuleDeviceVoltage) : V1: VMF R0/5 : sensor
              |
              +-7007 (cevSensorModuleDeviceVoltage) : V1: 12v R0/6 : sensor
              |
              +-7008 (cevSensorModuleDeviceVoltage) : V1: VDD R0/7 : sensor
              |
              +-7009 (cevSensorModuleDeviceVoltage) : V1: GP1 R0/8 : sensor
              |
              +-7010 (cevSensorModuleDeviceVoltage) : V1: GP2 R0/9 : sensor
              |
              +-7011 (cevSensorModuleDeviceTemp) : Temp: CPU R0/10 : sensor
              |
              +-7012 (cevSensorModuleDeviceTemp) : Temp: Outlet R0/11 : sensor
              |
              +-7013 (cevSensorModuleDeviceTemp) : Temp: Inlet R0/12 : sensor
              |
              +-7014 (cevSensorModuleDeviceTemp) : Temp: Asic1 R0/13 : sensor
              |
              +-7026 (cevModuleCpuType) : cpu R0/0 : other
              |
              +-7027 (cevPortUSB) : usb R0/0 : port
              |
              \-7029 (cevPortGe) : NME R0 : port

Mib Variables printed : <entPhysicalName entPhysicalClass>
```

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 "Enabling Notifications" section on page 4-2. 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 Quality of Service

This section provides the following information about using Quality of Service (QoS) in your configuration:

- CISCO-CLASS-BASED-QOS-MIB Overview
- Viewing QoS Configuration Settings Using the CISCO-CLASS-BASED-QOS-MIB
- Monitoring QoS Using the CISCO-CLASS-BASED-QOS-MIB
- Considerations for Processing QoS Statistics
- Sample QoS Applications

CISCO-CLASS-BASED-QOS-MIB Overview

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

CISCO-CLASS-BASED-QOS-MIB Object Relationship

To understand how to navigate the CISCO-CLASS-BASED-QOS-MIB tables, it is important to understand the relationship among different QoS objects. QoS objects consists of:

- Match Statement—specific match criteria to identify packets for classification purposes.
- Class Map—a user-defined traffic class that contains 1 or more match statements used to classify packets into different categories.
- Feature Action—a QoS feature. Features include police, traffic shaping, queueing, random detect, and packet marking. After the traffic has been classified we apply actions to each traffic class.
- Policy Map—a user-defined policy that associates a Qos feature action to the user-define class map.

- Service Policy—a policy map that has been attached to an interface.

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

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

QoS MIB Information Storage

CISCO-CLASS-BASED-QOS-MIB information is stored in:

- Configuration instances – includes all class maps, policy map, match statements, and feature action configuration parameters. Might have multiple identical instances. Multiple instances of the same QoS feature share a single configuration object, which is identified by cbQosConfigIndex.
- Runtime Statistics instances—Includes summary counts and rates by traffic class before and after any configured QoS policies are enforced. In addition, detailed feature-specific statistics are available for select PolicyMap features. Each has a unique runtime 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 configurations.

Viewing QoS Configuration Settings Using the CISCO-CLASS-BASED-QOS-MIB

This section contains examples that show how QoS configuration settings are stored in CISCO-CLASS-BASED-QOS-MIB tables. The samples show information grouped by QoS object; however, the actual output of an SNMP query might show QoS information similar to the following.

Note This is only a partial display of all QoS information.

```
getmany -v2c 9.0.0.55 ciscoCBQosMIB
cbQosIfType.64 = mainInterface(1)
cbQosIfType.66 = mainInterface(1)
cbQosPolicyDirection.64 = input(1)
cbQosPolicyDirection.66 = output(2)
cbQosIfIndex.64 = 4
cbQosIfIndex.66 = 4
cbQosFrDLCI.64 = 0
cbQosFrDLCI.66 = 0
cbQosAtmVPI.64 = 0
cbQosAtmVPI.66 = 0
cbQosAtmVCI.64 = 0
cbQosAtmVCI.66 = 0
cbQosEntityIndex.64 = 0
cbQosEntityIndex.66 = 0
cbQosConfigIndex.64.64 = 15348192
cbQosConfigIndex.64.7282691 = 12103539
cbQosConfigIndex.64.15123441 = 1593
cbQosConfigIndex.64.15755442 = 1594
cbQosConfigIndex.66.66 = 15889568
cbQosConfigIndex.66.1907619 = 15971699
cbQosConfigIndex.66.9319458 = 1594
cbQosConfigIndex.66.15082481 = 1593
cbQosObjectsType.64.64 = policymap(1)
cbQosObjectsType.64.7282691 = police(7)
cbQosObjectsType.64.15123441 = classmap(2)
cbQosObjectsType.64.15755442 = matchStatement(3)
cbQosObjectsType.66.66 = policymap(1)
cbQosObjectsType.66.1907619 = queueing(4)
cbQosObjectsType.66.9319458 = matchStatement(3)
cbQosObjectsType.66.15082481 = classmap(2)
cbQosParentObjectsIndex.64.64 = 0
cbQosParentObjectsIndex.64.7282691 = 15123441
cbQosParentObjectsIndex.64.15123441 = 64
cbQosParentObjectsIndex.64.15755442 = 15123441
cbQosParentObjectsIndex.66.66 = 0
cbQosParentObjectsIndex.66.1907619 = 15082481
cbQosParentObjectsIndex.66.9319458 = 15082481
cbQosParentObjectsIndex.66.15082481 = 66
cbQosPolicyMapName.15348192 = policy-police
cbQosPolicyMapName.15889568 = policy-bw
cbQosPolicyMapDesc.15348192 =
cbQosPolicyMapDesc.15889568 =
cbQosCMName.1593 = class-default
cbQosCMDesc.1593 =
cbQosCMInfo.1593 = matchAny(3)
.....
.....
```

Monitoring QoS Using the CISCO-CLASS-BASED-QOS-MIB

This section describes how to monitor QoS on the router by checking the QoS statistics in the CISCO-CLASS-BASED-QOS-MIB tables.

Note The CISCO-CLASS-BASED-QOS-MIB might contain more information than what is displayed in the output of CLI **show** commands.

Table A-1 lists the types of QoS statistics tables.

Table A-1 QoS Statistics Tables

QoS Table	Statistics
cbQosCMStatsTable	Class Map—Counts of packets, bytes, and bit rate before and after QoS policies are executed. Counts of dropped packets and bytes.
cbQosMatchStmtStatsTable	Match Statement—Counts of packets, bytes, and bit rate before executing QoS policies.
cbQosPoliceStatsTable	Police Action—Counts of packets, bytes, and bit rate that conforms to, exceeds, and violates police actions.
cbQosQueueingStatsTable	Queueing—Counts of discarded packets and bytes, and queue depths.

Table A-1 QoS Statistics Tables

QoS Table	Statistics
cbQosTSStatsTable	Traffic Shaping—Counts of delayed and dropped packets and bytes, the state of a feature, and queue size.
cbQosREDClassStatsTable	Random Early Detection—Counts of packets and bytes dropped when queues were full, and counts of bytes and octets transmitted.

Considerations for Processing QoS Statistics

The router maintains 64-bit counters for most QoS statistics. However, some QoS counters are implemented as a 32-bit counter with a 1-bit overflow flag. In the following samples, these counters are shown as 33-bit counters.

When accessing QoS counter statistics, consider the following:

- SNMPv2c or SNMPv3 applications—Access the entire 64 bits of the QoS counter through *cbQosxxx64* MIB objects.
- SNMPv1 applications—Access QoS statistics in the MIB as follows:
  - Access the lower 32 bits of the counter through cb*Qosxxx* MIB objects.
  - Access the upper 32 bits of the counter through *cbQosxxxOverflow* MIB objects.

Sample QoS Statistics Tables

The samples in this section show the counters in CISCO-CLASS-BASED-QOS-MIB statistics tables:

- Figure A-2 shows the counters in the cbQosCMStatsTable and the indexes for accessing these and other statistics.
- Figure A-3 shows the counters in cbQosMatchStmtStatsTable, cbQosPoliceStatsTable, cbQosQueueingStatsTable, cbQosTSStatsTable, and cbQosREDClassStatsTable.

For ease-of-use, the following figures show some counters as a single object even though the counter is implemented as three objects. For example, `cbQosCMPrePolicyByte` is implemented as:

- cbQosCMPrePolicyByteOverflow
- cbQosCMPrePolicyByte
- cbQosCMPrePolicyByte64

Figure A-2 QoS Class Map Statistics and Indexes

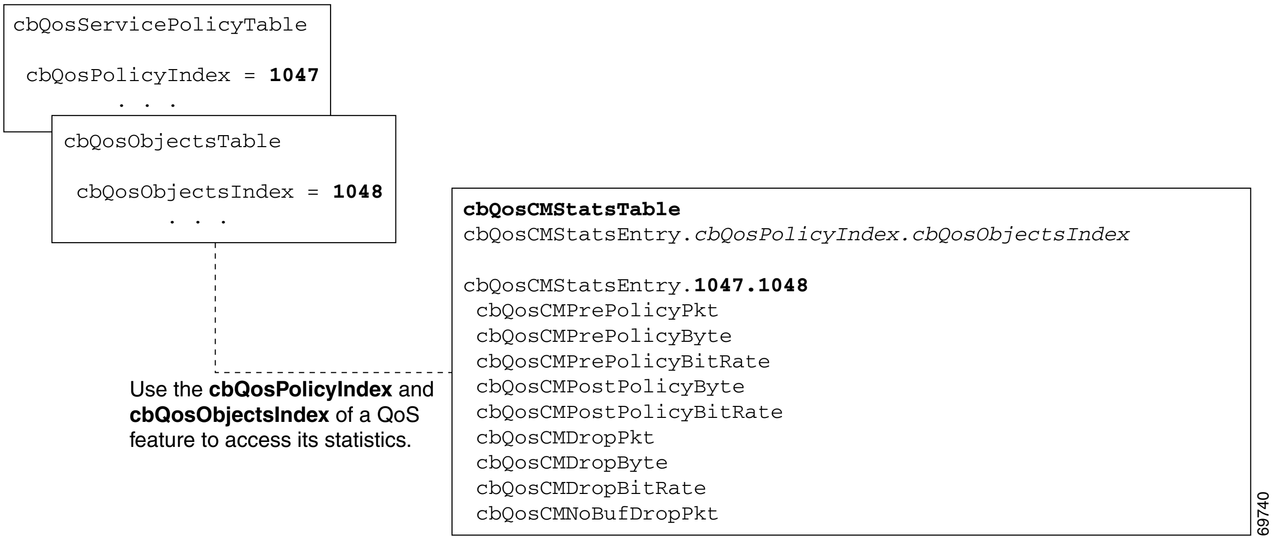
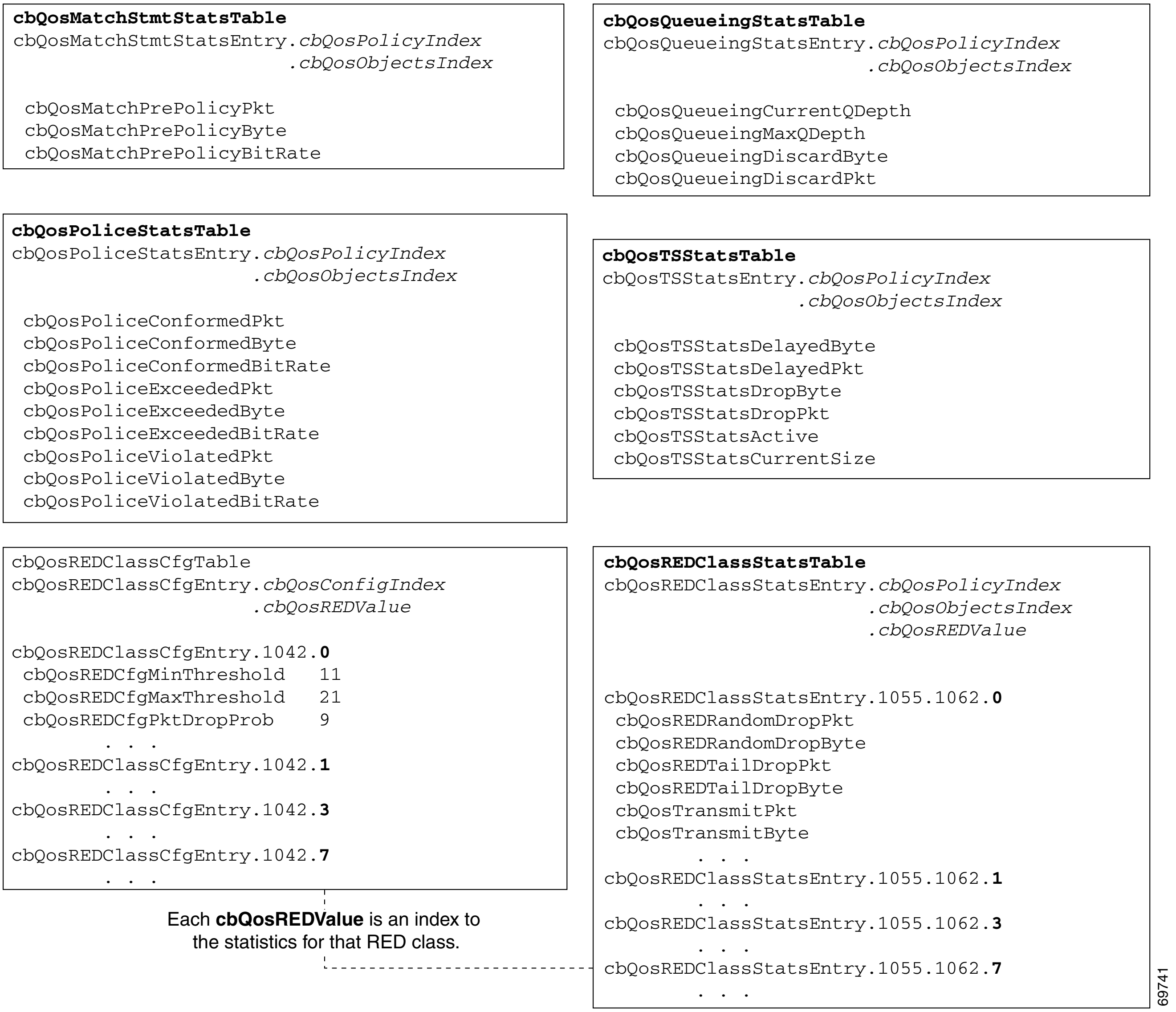


Figure A-3 QoS Statistics Tables



```
cbQosMatchStmtStatsTable
cbQosMatchStmtStatsEntry.cbQosPolicyIndex
                        .cbQosObjectsIndex

 cbQosMatchPrePolicyPkt
 cbQosMatchPrePolicyByte
 cbQosMatchPrePolicyBitRate
```

```
cbQosQueueingStatsTable
cbQosQueueingStatsEntry.cbQosPolicyIndex
                       .cbQosObjectsIndex

 cbQosQueueingCurrentQDepth
 cbQosQueueingMaxQDepth
 cbQosQueueingDiscardByte
 cbQosQueueingDiscardPkt
```

```
cbQosPoliceStatsTable
cbQosPoliceStatsEntry.cbQosPolicyIndex
                     .cbQosObjectsIndex

 cbQosPoliceConformedPkt
 cbQosPoliceConformedByte
 cbQosPoliceConformedBitRate
 cbQosPoliceExceededPkt
 cbQosPoliceExceededByte
 cbQosPoliceExceededBitRate
 cbQosPoliceViolatedPkt
 cbQosPoliceViolatedByte
 cbQosPoliceViolatedBitRate
```

```
cbQosTSStatsTable
cbQosTSStatsEntry.cbQosPolicyIndex
                 .cbQosObjectsIndex

 cbQosTSStatsDelayedByte
 cbQosTSStatsDelayedPkt
 cbQosTSStatsDropByte
 cbQosTSStatsDropPkt
 cbQosTSStatsActive
 cbQosTSStatsCurrentSize
```

```
cbQosREDClassCfgTable
cbQosREDClassCfgEntry.cbQosConfigIndex
                     .cbQosREDValue

cbQosREDClassCfgEntry.1042.0
 cbQosREDCfgMinThreshold   11
 cbQosREDCfgMaxThreshold   21
 cbQosREDCfgPktDropProb    9
        . . .
cbQosREDClassCfgEntry.1042.1
        . . .
cbQosREDClassCfgEntry.1042.3
        . . .
cbQosREDClassCfgEntry.1042.7
        . . .
```

```
cbQosREDClassStatsTable
cbQosREDClassStatsEntry.cbQosPolicyIndex
                       .cbQosObjectsIndex
                       .cbQosREDValue


cbQosREDClassStatsEntry.1055.1062.0
 cbQosREDRandomDropPkt
 cbQosREDRandomDropByte
 cbQosREDTailDropPkt
 cbQosREDTailDropByte
 cbQosTransmitPkt
 cbQosTransmitByte
        . . .
cbQosREDClassStatsEntry.1055.1062.1
        . . .
cbQosREDClassStatsEntry.1055.1062.3
        . . .
cbQosREDClassStatsEntry.1055.1062.7
        . . .
```

Each **cbQosREDValue** is an index to the statistics for that RED class.

* Counts in cbQosREDClassStatsTable are maintained per class, not cbQosREDValue. All instances of a counter that have the same cbQosREDValue also have the same count.

Sample QoS Applications

This section presents examples of code showing how to retrieve information from the CISCO-CLASS-BASED-QOS-MIB to use for QoS billing operations. You can use these examples to help you develop billing applications. The topics include:

- Checking Customer Interfaces for Service Policies

- Retrieving QoS Billing Information

Checking Customer Interfaces for Service Policies

This section describes a sample algorithm that checks the CISCO-CLASS-BASED-QOS-MIB for customer interfaces with service policies, and marks those interfaces for further application processing (such as billing for QoS services).

The algorithm uses two SNMP **get-next** requests for each customer interface. For example, if the router has 2000 customer interfaces, 4000 SNMP **get-next** requests are required to determine if those interfaces have transmit and receive service policies associated with them.

Note This algorithm is for informational purposes only. Your application needs may be different.

Check the MIB to see which interfaces are associated with a customer. Create a pair of flags to show if a service policy has been associated with the transmit and receive directions of a customer interface. Mark noncustomer interfaces TRUE (so no more processing is required for them).

```
FOR each ifEntry DO
  IF (ifEntry represents a customer interface) THEN
     servicePolicyAssociated[ifIndex].transmit = FALSE;
     servicePolicyAssociated[ifIndex].receive = FALSE;
  ELSE
     servicePolicyAssociated[ifIndex].transmit = TRUE;
     servicePolicyAssociated[ifIndex].receive = TRUE;
  END-IF
END-FOR
```

Examine the cbQosServicePolicyTable and mark each customer interface that has a service policy attached to it. Also note the direction of the interface.

```
x = 0;
done = FALSE;
WHILE (!done)
  status = snmp-getnext (
           ifIndex = cbQosIfIndex.x,
           direction = cbQosPolicyDirection.x
  );
  IF (status != 'noError') THEN
     done = TRUE
  ELSE
     x = extract cbQosPolicyIndex from response;
     IF (direction == 'output') THEN
       servicePolicyAssociated[ifIndex].transmit = TRUE;
     ELSE
       servicePolicyAssociated[ifIndex].receive = TRUE;
     END-IF
  END-IF
END-WHILE
```

Manage cases in which a customer interface does not have a service policy attached to it.

```
FOR each ifEntry DO
  IF (!servicePolicyAssociated[ifIndex].transmit) THEN
     Perform processing for customer interface without a transmit service policy.
  END-IF
  IF (!servicePolicyAssociated[ifIndex].receive) THEN
     Perform processing for customer interface without a receive service policy.
  END-IF
END-FOR
```

Retrieving QoS Billing Information

This section describes a sample algorithm that uses the CISCO-CLASS-BASED-QOS-MIB for QoS billing operations. The algorithm periodically retrieves post-policy input and output statistics, combines them, and sends the result to a billing database.

The algorithm uses the following:

- One SNMP **get** request per customer interface—to retrieve the ifAlias.
- Two SNMP **get-next** requests per customer interface—to retrieve service policy indexes.
- Two SNMP **get-next** requests per customer interface for each object in the policy—to retrieve post-policy bytes. For example, if there are 100 interfaces and 10 objects in the policy, the algorithm requires 2000 **get-next** requests (2 x 100 x 10).

Note This algorithm is for informational purposes only. Your application needs may be different.

Set up customer billing information.

```
FOR each ifEntry DO
  IF (ifEntry represents a customer interface) THEN
     status = snmp-getnext (id = ifAlias.ifIndex);
     IF (status != ‘noError’) THEN
         Perform error processing.
     ELSE
        billing[ifIndex].isCustomerInterface = TRUE;
        billing[ifIndex].customerID = id;
        billing[ifIndex].transmit   = 0;
        billing[ifIndex].receive    = 0;
     END-IF
  ELSE
     billing[ifIndex].isCustomerInterface = FALSE;
  END-IF
END-FOR
```

Retrieve billing information.

```
x = 0;
done = FALSE;
WHILE (!done)
  response = snmp-getnext (
             ifIndex = cbQosIfIndex.x,
             direction = cbQosPolicyDirection.x
  );
  IF (response.status != ‘noError’) THEN
     done = TRUE
  ELSE
     x = extract cbQosPolicyIndex from response;
     IF (direction == ‘output’) THEN
        billing[ifIndex].transmit = GetPostPolicyBytes (x);
     ELSE
        billing[ifIndex].receive = GetPostPolicyBytes (x);
     END-IF
  END-IF
END-WHILE
```

Determine the number of post-policy bytes for billing purposes.

```
GetPostPolicyBytes (policy)
  x = policy;
  y = 0;
```

```
     total = 0;
     WHILE (x == policy)
        response = snmp-getnext (type = cbQosObjectsType.x.y);
        IF (response.status == ‘noError’)
           x = extract cbQosPolicyIndex from response;
           y = extract cbQosObjectsIndex from response;
           IF (x == policy AND type == ‘classmap’)
              status = snmp-get (bytes = cbQosCMPostPolicyByte64.x.y);
              IF (status == ‘noError’)
                      total += bytes;
              END-IF
           END-IF
        END-IF
     END-WHILE
   RETURN total;
```

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-33 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-34.

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 and QoS data information to determine the amount to bill customers for traffic. It also includes a scenario for demonstrating that a QoS service policy attached to an interface is policing traffic on that interface.

This section contains the following topics:

- Input and Output Interface Counts, page A-34
- Determining the Amount of Traffic to Bill to a Customer, page A-35
- Scenario for Demonstrating QoS Traffic Policing, page A-35

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 3-109.

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

- Unless noted, all IF-MIB counters are supported on Cisco ASR 1000 Series Routers interfaces.
- For IF-MIB high capacity counter support, Cisco conforms 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.

- When a QoS service policy is attached to an interface, the router applies the rules of the policy to traffic on the interface and increments the packet and bytes counts on the interface.

The following CISCO-CLASS-BASED-QOS-MIB objects provide interface counts:

- cbQosCMDropPkt and cbQosCMDropByte (cbQosCMStatsTable)—Total number of packets and bytes that were dropped because they exceeded the limits set by the service policy. These counts include only those packets and bytes that were dropped because they exceeded service policy limits. The counts do not include packets and bytes dropped for other reasons.
- cbQosPoliceConformedPkt and cbQosPoliceConformedByte (cbQosPoliceStatsTable)—Total number of packets and bytes that conformed to the limits of the service policy and were transmitted.

Determining the Amount of Traffic to Bill to a Customer

Perform these steps to determine how much traffic on an interface is billable to a particular customer:

Step 1 Determine which service policy on the interface applies to the customer.

Step 2 Determine the index values of the service policy and class map used to define the customer’s traffic. You need this information in the following steps.

Step 3 Generate traffic with the traffic generator. The data rate should be more than that is configured for Conform burst(bc)/Exceed burst(be) for the policy.

Step 4 (Optional) Access the cbQosCMDropPkt object (cbQosCMStatsTable) for the customer to determine how much of the customer’s traffic was dropped because it exceeded service policy limits.

Scenario for Demonstrating QoS Traffic Policing

This section describes a scenario that demonstrates the use of SNMP QoS statistics to determine how much traffic on an interface is billable to a particular customer. It also shows how packet counts are affected when a service policy is applied to traffic on the interface.

To create the scenario, follow these steps, each of which is described in the sections that follow:

1. Create and attach a service policy to an interface.
2. View packet counts before the service policy is applied to traffic on the interface.
3. Issue a **`ping`** command to generate traffic on the interface. Note that the service policy is applied to the traffic.
4. View packet counts after the service policy is applied to determine how much traffic to bill the customer for:
   - Conformed packets—The number of packets within the range set by the service policy and for which you can charge the customer.
   - Exceeded or dropped packets—The number of packets that were not transmitted because they were outside the range of the service policy. These packets are not billable to the customer.

Note In the above scenario, the Cisco ASR 1000 Series Routers is used as an interim device (that is, traffic originates elsewhere and is destined for another device).

Service Policy Configuration

This scenario uses the following policy-map configuration. For information on how to create a policy map, see “Configuring Quality of Service” in the *Cisco ASR 1000 Series Router Software Configuration Guide*.

```
Policy Map test-police
    Class class-default
     police cir 1000000 bc 10000 be 20000
       conform-action transmit
       exceed-action drop
       violate-action drop

interface GigabitEthernet1/1/5
 ip address 15.1.0.52 255.0.0.0
 no negotiation auto
 service-policy output test-police
end
```

Packet Counts Before the Service Policy Is Applied

The following CLI and SNMP output shows the interface’s output traffic before the service policy is applied:

CLI Command Output

```
Router#sh policy-map interface gi 1/1/5

 GigabitEthernet1/1/5

  Service-policy output: test-police

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 1000000 bps, bc 10000 bytes, be 20000 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
```

SNMP Output

```
ptolemy:4> getmany 9.0.0.52 cbQosIfIndex
cbQosIfIndex.290 = 18
ptolemy:5> getone 9.0.0.52 ifDescr.18
ifDescr.18 = GigabitEthernet1/1/5
ptolemy:6>

getmany 9.0.0.52 cbQosCMDropPkt cbQosCMDropByte
cbQosCMDropPkt.290.9756705 = 0
cbQosCMDropByte.290.9756705 = 0
ptolemy:77>
```

Packet Counts After the Service Policy Is Applied

After you generate traffic using the traffic generator, look at the number of packets that exceeded and conformed to the committed information rate (CIR) set by the **`police`** command:

- 19351 packets conformed to the police rate and were transmitted
- 80 packets exceeded the police rate and were dropped
- 16066130 packets violated the police rate and were dropped

The following CLI and SNMP output show the counts on the interface after the service policy is applied. The object cbQosCMDropPkt refers to sum of exceeded and violated packets and cbQosCMDropByte refers to the sum of exceeded and violated bytes. (In the output, exceeded andviolated packet counts are shown in boldface.)

CLI Command Output

```
Router#sh show policy-map int gi 1/1/5

 GigabitEthernet1/1/5

  Service-policy output: test-police

    Class-map: class-default (match-any)
      16085561 packets, 1994609369 bytes

      5 minute offered rate 16051000 bps, drop rate 16032000 bps
      Match: any
      police:
          cir 1000000 bps, bc 10000 bytes, be 10000 bytes
        conformed 19351 packets, 2399329 bytes; actions:
          transmit
        exceeded 80 packets, 9920 bytes; actions:
          drop
        violated 16066130 packets, 1992200120 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 16032000 bps
Router#
```

SNMP Output

```
getmany 9.0.0.52 cbQosCMDropPkt cbQosCMDropByte
cbQosCMDropPkt.290.9756705 = 16066210
cbQosCMDropByte.290.9756705 = 1992210040
ptolemy:77>
        . . .
```

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-2 lists capacity counter object identifiers (OIDs).

Table A-2 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 MIB Tools from the following URL:

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

Overview of SIPs and SPAs

The following list describes some of the general characteristics of Cisco SIPs and SPAs (shared port adapter).

- A Cisco ASR 1000 Series SPA Interface Processor (SIP) is a carrier card that:
  - Inserts into a router slot like a line card. It provides no network connectivity on its own.
  - Contains one or more subslots, which are used to house one or more SPAs. The SPA provides interface ports for network connectivity.

- Resides in the router fully populated either with functional SPAs in all subslots during normal operation or with a blank filler plate (SPA-BLANK=) inserted in all empty subslots.
- Support online insertion and removal (OIR) with SPAs inserted in their subslots. SPAs also support OIR and can be inserted or removed independently from the SIP.

- A Shared Port Adapter (SPA) is a modular type of port adapter that:
  - Inserts into a subslot of a compatible SIP carrier card to provide network connectivity and increased interface port density. A SIP can hold one or more SPAs, depending on the SIP type.
  - Provides services rather than network connectivity and insert into subslots of compatible cards. For example, the IPSec VPN SPA provides services such as IP Security (IPSec) encryption/decryption, generic routing encapsulation (GRE), and Internet Key Exchange (IKE) key generation.
  - Are available in single-height (inserts into one SIP subslot) and double-height (inserts into two single, vertically aligned SIP subslots).

Note SPA-1X10GE-WL-V2 is supported on the Cisco ASR1K platform begining with Cisco IOS XE Release 3.3.0 S and Cisco IOS Release 15.1(2)S.

Note The 1-Port 10GE LAN/WAN-PHY Shared Port Adapter (SPA-1X10GE-WL-V2) should be on the same mode, either the LAN mode or the WAN mode, at both ends.

Note The SPA-1X10GE-WL-V2 (configured in the LAN mode) is compatible with the SPA-1X10GE-L-V2 (LAN SPA).

Configuring the LAN-PHY Mode

Use the following commands to configure the LAN-PHY mode on the 1-Port 10GE LAN/WAN-PHY Shared Port Adapter (SPA-1X10GE-WL-V2):

```
show controllers wanphy interface-path-id [alarms | all | registers]
configure terminal
controller wanphy interface-path-id
lanmode on
end
hw-module subslot interface-path-id reload
show controllers wanphy interface-path-id [alarms | all | registers]
```

Note After configuring the LAN-PHY mode and reloading the SPA, all the links are in the UP state.

Note Effective from Cisco IOS Release 15.1(2)S, 1-Port 10GE LAN/WAN-PHY Shared Port Adapter (SPA-1X10GE-WL-V2) supports both the LAN and WAN modes.

Displaying the SIP Hardware Type

To verify the SIP hardware type that is installed in your Cisco ASR 1000 series router, you can use the show platform command. There are some commands on the Cisco ASR 1000 series router that provide SIP hardware information. There are more sub-commands which give detailed output for each SIP/SPA card. The example below shows some list of such commands.

Example A-9 Example of the show platform command

The following example shows the output of the **show platform** command on the Cisco ASR 1000 Series Routers:

```
Router#sh platform

Chassis type: ASR1006


Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-SIP10       ok                    06:19:03
 0/0      SPA-1XOC12-POS      ok                    06:17:25
 0/1      SPA-2XCT3/DS0       ok                    06:17:25
 0/2      SPA-2XT3/E3         ok                    06:17:25
 0/3      SPA-8X1GE-V2        ok                    06:17:34
1         ASR1000-SIP10       ok                    06:19:03
 1/0      SPA-1X10GE-L-V2     ok                    06:17:36
 1/1      SPA-5X1GE-V2        ok                    06:17:25
 1/2      SPA-8X1FE-TX-V2     ok                    06:17:36
2         ASR1000-SIP10       ok                    06:19:03
 2/0      SPA-2X1GE-V2        ok                    06:17:36
 2/1      SPA-10X1GE-V2       ok                    06:17:36
 2/2      SPA-2XOC3-POS       ok                    06:17:36
R0        ASR1000-RP1         ok, active            06:19:03
R1                            unknown               06:19:03
F0        ASR1000-ESP10       ok, active            06:19:03
P0        ASR1006-PWR-AC      ok                    06:18:25
P1        ASR1006-FAN         ok                    06:18:25


Slot      CPLD Version        Firmware Version
--------- ------------------- ---------------------------------------
0         06120701            12.2(20070802:195019) [gschnorr-mcp_...
1         06120701            12.2(20070802:195019) [gschnorr-mcp_...
2         06120701            12.2(20070802:195019) [gschnorr-mcp_...
```

```
R0        0706210B            12.2(20070807:170946) [gschnorr-mcp_...

R1        N/A                 N/A

F0        07021400            12.2(20070802:195019) [gschnorr-mcp_...




Router#sh platform ?

  hardware  Show platform hardware information

  software  Show platform software information

  |         Output modifiers

  <cr>


Router#sh platform har

Router#sh platform hardware ?

  cpp        Cisco packet processor

  interface  Interface information

  port       port information

  slot       Slot information

  subslot    Subslot information


Router#sh platform hardware slot ?

  0   SPA-Inter-Processor slot 0

  1   SPA-Inter-Processor slot 1

  2   SPA-Inter-Processor slot 2

  F0  Embedded-Service-Processor slot 0

  F1  Embedded-Service-Processor slot 1

  R0  Route-Processor slot 0

  R1  Route-Processor slot 1


Router#sh platform hardware slot 0 ?

  dram     MCP85xx DRAM commands

  eobc     Show EOBC

  fan      Fan commands

  io-port  IO Port information

  led      LED-related commands

  mcu      MCU related commands

  plim     PLIM information

  sensor   Sensor information
  serdes   Serdes information

  spa      SPA related information

  voltage  Voltage commands


Router#
```

APPENDIX B

QoS MIB Implementation

This appendix provides information about QoS-based features that are implemented on Cisco ASR 1000 Series Router line cards and what tables and objects in the QoS MIB support these QoS features. The Cisco ASR 1000 Series Routers FlexWAN and OSM line card families each have a different QoS implementation. Do not assume that the QoS features across line card families are equivalent. Some of the QOS configuration is done at the PFC2 (policy feature card) level and others at the parallel express forwarding (PXF) processor level in each line card.

This appendix contain the following topics:

Note For detailed Cisco Quality of Service (QoS) information, Cisco IOS QoS features, and the technologies that implement them, go to the following URL http://www.cisco.com/en/US/docs/ios/12_1/qos/configuration/guide/qcdintro.html

Implementing CISCO-CLASS-BASED-QOS-MIB

This section describes which objects from the CISCO-CLASS-BASED-QOS-MIB are implemented, which objects are relevant to the features available for Cisco ASR 1000 Series Routers line cards, and which QoS features are supported by each Cisco ASR 1000 Series Routers line card.

Table B-1 defines the expected values for Policy Actions.

Table B-1 QoS Policy Action Parameters

Policy Action	Definition	Notes
Bandwidth	A rate limiting function. The difference between the highest and lowest frequencies available for network signals. Bandwidth divides the link bandwidth among different traffic streams into multiple queues.	Must be set before you enable WRED. Aggregate bandwidth rate limits match all of the packets on an interface or subinterface. Granular bandwidth rate limits match a particular type of traffic based on precedence, MAC address, or other parameters.
Priority	Priority queuing allows you to assign a guaranteed minimum bandwidth to one queue to minimize the packet delay variance for delay-sensitive traffic.	A routing feature in which frames in an output queue are prioritized based on various characteristics, such as packet size and interface type.
Shape	A shaper typically delays excess traffic using a buffer or queueing mechanism, to hold packets and shape the flow when the data rate of the source is higher than expected. (For example, GTS uses a weighted fair queue to delay packets to shape the flow, and FRTS uses either a priority queue (PQ), a custom queue (CQ), or a first-in, first-out (FIFO) queue for the same, depending on how you configure it.)	Shapers identify traffic descriptor violations.
Police	A policer typically drops traffic. (For example, CAR's rate-limiting policer either drops the packet or rewrites its IP precedence, resetting the packet header's type of service bits.)	Policing is the process by which the OSR limits the bandwidth consumed by a flow of traffic. Policing can mark or drop traffic.

Table B-1 QoS Policy Action Parameters (continued)

Policy Action	Definition	Notes
Queue-limit	Parameter specifies the number of packets held by the queue. It operates on the default packet drop method of congestion management.	A Cisco queuing technique. A flow-based queuing algorithm that creates bit-wise fairness by allowing each queue to be serviced fairly in terms of byte count. For example, if queue 1 has 100-byte packets and queue 2 has 50-byte packets, the WFQ algorithm takes two packets from queue 2 for each one packet from queue 1. This makes service fair for each queue: 100 bytes each time the queue is serviced. WFQ ensures that queues do not starve for bandwidth and that traffic gets predictable service. Low-volume traffic streams–which comprise the majority of traffic–receive increased service, transmitting the same number of bytes as high-volume streams. This behavior results in what appears to be preferential treatment for low-volume traffic, when in actuality it is creating fairness.
Fair-queue	Traffic shaping smooths traffic by storing traffic above the configured rate in a queue. When a packet arrives at the interface for transmission, the following happens: • If the queue is empty, the arriving packet is processed by the traffic shaper. • If possible, the traffic shaper sends the packet. Otherwise, the packet is placed in the queue. • If the queue is not empty, the packet is placed in the queue. When there are packets in the queue, the traffic shaper removes the number of packets it can transmit from the queue at each time interval.	A Cisco queuing technique. A flow-based queuing algorithm that creates bit-wise fairness by allowing each queue to be serviced fairly in terms of byte count. For example, if queue 1 has 100-byte packets and queue 2 has 50-byte packets, the WFQ algorithm takes two packets from queue 2 for each one packet from queue 1. This makes service fair for each queue: 100 bytes each time the queue is serviced.

Table B-1 QoS Policy Action Parameters (continued)

Policy Action	Definition	Notes
WRED—weighted random early detection	Action that randomly discards packets during IP precedence settings congestion.	Precedence is a value of 0 to 7 where zero is low priority traffic and 7 represents high priority traffic.
Set (precedence)	The IP precedence (QoS) bits in the packet header are rewritten. The packet is then transmitted. You can use this action to either color (set precedence) or recolor (modify existing packet precedence) the packet.	—

Note Congestion-management tools include priority queuing (PQ), custom queuing (CQ), weighted fair queuing (WFQ), and class-based weighted fair queuing (CBWFQ).

Note Police and shape are traffic regulation mechanisms:

Shaping is used to create a traffic flow that limits the full bandwidth potential of the flows. This is used many times to prevent the overflow problem mentioned in the introduction. For instance, many network topologies use Frame Relay in a hub-and-spoke design. In this case, the central site normally has a high-bandwidth link (such as, T1), while remote sites have a low-bandwidth link in comparison (such as, 384 Kbps). In this case, it is possible for traffic from the central site to overflow the low bandwidth link at the other end. Shaping is a good way to pace traffic closer to 384 Kbps to avoid the overflow of the remote link. Traffic above the configured rate is buffered for transmission later to maintain the rate configured.

Policing is similar to shaping, but it differs in one important way; traffic that exceeds the configured rate is not buffered (and normally is discarded).

QoS MIB Policy Action Support Matrix

The tables in this section describe which objects from the CISCO-CLASS-BASED-QOS-MIB are implemented and which one are relevant to the different features available for Cisco ASR 1000 Series Routers line cards. The tables are divided into objects on the Cisco ASR 1000 Series Routers platform that are:

- Supported, implemented, and instrumented (works as defined in the MIB)—Table B-3
- Not supported or support is limited—Table B-4

Table B-2 lists the definitions of the values that are returned by objects listed in Table B-3 and Table B-4. Policy actions are dependent on return values.

Table B-2 QoS Table Return Values

Definition	Identifier
Returns valid data.	Value is V.
Returns invalid data	Value is I. The object is not supported by this platform.
Not instantiated (Does not instantiate (return) any value for this object.)	Value is a dash '–'.

Table B-3 lists QoS MIB table objects that are supported and implemented on the Cisco ASR 1000 Series Routers platform and the QoS policy actions that these objects support.

Table B-3 Supported QoS MIB Objects

	Policy Actions								
MIB Tables and Objects	**Band-width**	**Priority**	**Shape**	**Police**	**Queue Limit**	**Fair Queue**	**WRED**	**Set**	**Notes**
cbQosCMStatsTable									earl 6 (Sup2) only support packet counters and earl 7 (Sup3) only support byte counters.
cbQosCMPrePolicyPkt Overflow	V	V	V	V	V	V	V	V	The objects listed with a value of V (valid) are supported and return valid data.
cbQosCMPrePolicyPkt	V	V	V	V	V	V	V	V	
cbQosCMPrePolicyPkt64	V	V	V	V	V	V	V	V	
cbQosCMPrePolicyByte Overflow	V	V	V	V	V	V	V	V	
cbQosCMPrePolicyByte	V	V	V	V	V	V	V	V	
cbQosCMPrePolicyByte64	V	V	V	V	V	V	V	V	
cbQosCMPrePolicyBitRate	V	V	V	V	V	V	V	V	
cbQosCMPostPolicyByte Overflow	V	V	V	V	V	V	V	V	
cbQosCMPostPolicyByte	V	V	V	V	V	V	V	V	
cbQosCMPostPolicy Byte64	V	V	V	V	V	V	V	V	
cbQosCMPostPolicyBit Rate	V	V	V	V	V	V	V	V	
cbQosCMDropPkt Overflow	V	V	V	V	V	V	V	V	
cbQosCMDropPkt	V	V	V	V	V	V	V	V	
cbQosCMDropPkt64	V	V	V	V	V	V	V	V	

Table B-3 Supported QoS MIB Objects (continued)

MIB Tables and Objects	Policy Actions								Notes
	Bandwidth	Priority	Shape	Police	Queue Limit	Fair Queue	WRED	Set	
cbQosCMDropByteOverflow	V	V	V	V	V	V	V	V	
cbQosCMDropByte	V	V	V	V	V	V	V	V	
cbQosCMDropByte64	V	V	V	V	V	V	V	V	
cbQosCMDropBitRate	V	V	V	V	V	V	V	V	
cbQosMatchStmtStatsTable									earl 6 (Sup2) only support packet counters and earl 7 (Sup3) only support byte counters.
cbQosMatchPrePolicyPktOverflow	I	I	I	V	I	I	I	I	The objects listed with a value of I (invalid) are supported but return invalid data for all actions except for **Police action** (the return data is valid).
cbQosMatchPrePolicyPkt	I	I	I	V	I	I	I	I	
cbQosMatchPrePolicyPkt64	I	I	I	V	I	I	I	I	
cbQosMatchPrePolicyByteOverflow	I	I	I	V	I	I	I	I	
cbQosMatchPrePolicyByte	I	I	I	V	I	I	I	I	
cbQosMatchPrePolicyBitRate	I	I	I	V	I	I	I	I	
cbQosMatchPrePolicyByte64	I	I	I	V	I	I	I	I	
cbQosPoliceStatsTable									earl 6 (Sup2) only support packet counters and earl 7 (Sup3) only support byte counters.
cbQosPoliceConformedPktOverflow	–	–	–	V	–	–	–	–	The objects listed are supported but only return V (valid) data for Police action.
cbQosPoliceConformedPkt	–	–	–	V	–	–	–	–	

Table B-3 Supported QoS MIB Objects (continued)

	Policy Actions								
MIB Tables and Objects	**Band-width**	**Priority**	**Shape**	**Police**	**Queue Limit**	**Fair Queue**	**WRED**	**Set**	**Notes**
cbQosPoliceConformedPkt64	–	–	–	V	–	–	–	–	The objects listed are supported but only return V (valid) data for Police action.
cbQosPoliceConformedByteOverflow	–	–	–	V	–	–	–	–	
cbQosPoliceConformedByte	–	–	–	V	–	–	–	–	
cbQosPoliceConformedByte64	–	–	–	V	–	–	–	–	
cbQosPoliceConformedBitRate	–	–	–	V	–	–	–	–	
cbQosPoliceExceededPktOverflow	–	–	–	V	–	–	–	–	
cbQosPoliceExceededPkt	–	–	–	V	–	–	–	–	
cbQosPoliceExceededPkt64	–	–	–	V	–	–	–	–	
cbQosPoliceExceededByteOverflow	–	–	–	V	–	–	–	–	
cbQosPoliceExceededByte	–	–	–	V	–	–	–	–	
cbQosPoliceExceededByte64	–	–	–	V	–	–	–	–	
cbQosPoliceExceededBitRate	–	–	–	V	–	–	–	–	
cbQosQueueingCfgTable									
cbQosQueueingCfgFlowEnabled	–	–	–	–	–	V	–	–	Not supported. Always false(2).
cbQosQueueingCfgIndividualQSize	–	–	–	–	–	–	–	–	Not supported. Always 0.
cbQosQueueingCfgDynamicQNumber	–	–	–	–	–	–	–	–	Not supported. Always 0.
cbQosQueueingStatsTable									
cbQosQueueingCurrentQDepth	V	V	–	–	V	V	–	–	The objects listed are supported but return valid data only for Bandwidth, Priority, Queue Limit, and Fair Queue.

Table B-3 Supported QoS MIB Objects (continued)

MIB Tables and Objects	Policy Actions								Notes
	Band-width	Priority	Shape	Police	Queue Limit	Fair Queue	WRED	Set	
cbQosQueueingMaxQDepth	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardByteOverflow	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardByte	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardByte64	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardPktOverflow	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardPkt	V	V	–	–	V	V	–	–	
cbQosQueueingDiscardPkt64	V	V	–	–	V	V	–	–	
cbQosTSStatsTable									The objects listed are supported and return valid data for only Shape, Queue Limit, Fair Queue, and WRED.
cbQosTSStatsDropByteOverflow	–	–	V	–	V	V	V	–	
cbQosTSStatsDropByte	–	–	V	–	V	V	V	–	
cbQosTSStatsDropByte64	–	–	V	–	V	V	V	–	
cbQosTSStatsDropPktOverflow	–	–	V	–	V	V	V	–	
cbQosTSStatsDropPkt	–	–	V	–	V	V	V	–	
cbQosTSStatsDropPkt64	–	–	V	–	V	V	V	–	
cbQosTSStatsCurrentQSize	–	–	V	–	V	V	V	–	
cbQosREDClassStatsTable									Not instantiated for shape even though the CLI shows values for random and tail counters.
cbQosREDRandomDropPktOverflow	–	–	–	–	–	–	V	–	These objects are supported and return valid data for WRED action only.
cbQosREDRandomDropPkt	–	–	–	–	–	–	V	–	
cbQosREDRandomDropPkt64	–	–	–	–	–	–	V	–	

Table B-3 Supported QoS MIB Objects (continued)

MIB Tables and Objects	Policy Actions								Notes
	Band-width	Priority	Shape	Police	Queue Limit	Fair Queue	WRED	Set	
cbQosREDRandomDropByteOverflow	–	–	–	–	–	–	V	–	
cbQosREDRandomDropByte	–	–	–	–	–	–	V	–	
cbQosREDRandomDropByte64	–	–	–	–	–	–	V	–	
cbQosREDTailDropPktOverflow	–	–	–	–	–	–	V	–	
cbQosREDTailDropPkt	–	–	–	–	–	–	V	–	These objects are supported and return valid data for WRED action only.
cbQosREDTailDropPkt64	–	–	–	–	–	–	V	–	
cbQosREDTailDropByteOverflow	–	–	–	–	–	–	V	–	
cbQosREDTailDropByte	–	–	–	–	–	–	V	–	
cbQosREDTailDropByte64	–	–	–	–	–	–	V	–	
cbQosREDTransmitPktOverflow	–	–	–	–	–	–	V	–	
cbQosREDTransmitPkt	–	–	–	–	–	–	V	–	
cbQosREDTransmitPkt64	–	–	–	–	–	–	V	–	
cbQosREDTransmitByteOverflow	–	–	–	–	–	–	V	–	
cbQosREDTransmitByte	–	–	–	–	–	–	V	–	
cbQosREDTransmitByte64	–	–	–	–	–	–	V	–	

Table B-4 lists QoS MIB table objects that are unsupported or have limited support on the Cisco ASR 1000 Series Routers platform and the QoS policy actions that these objects support.

Table B-4 QoS MIB Objects—Unsupported or Limited Support

	Policy Actions								
MIB Tables and Objects	**Band-width**	**Priority**	**Shape**	**Police**	**Queue Limit**	**Fair Queue**	**WRED**	**Set**	**Notes**
cbQosCMStatsTable									The objects listed are not supported but do return valid data which is always zero (0).
cbQosCMNoBufDropPkt Overflow	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	
cbQosCMNoBufDropPkt	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	
cbQosCMNoBufDrop Pkt64	**V**	**V**	**V**	**V**	**V**	**V**	**V**	**V**	
cbQosPoliceStatsTable									The objects listed are not supported but do return valid data for Police action which is always zero (0).
cbQosPoliceViolatedPkt Overflow	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolatedPkt	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolatedPkt64	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolated ByteOverflow	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolatedByte	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolated Byte64	–	–	–	**V**	–	–	–	–	
cbQosPoliceViolated BitRate	–	–	–	**V**	–	–	–	–	
cbQosTSStatsTable									The objects listed are not supported but do return valid data which is always zero (0) for Shape, Queue Limit, Fair Queue, and WRED.
cbQosTSStatsDelayed ByteOverflow	–	–	**V**		**V**	**V**	**V**	–	
cbQosTSStatsDelayedByte	–	–	**V**		**V**	**V**	**V**	–	
cbQosTSStatsDelayed Byte64	–	–	**V**		**V**	**V**	**V**	–	
cbQosTSStatsDelayed PktOverflow	–	–	**V**		**V**	**V**	**V**	–	

Table B-4 QoS MIB Objects—Unsupported or Limited Support (continued)

MIB Tables and Objects	Policy Actions								Notes
	Band-width	Priority	Shape	Police	Queue Limit	Fair Queue	WRED	Set	
cbQosTSStatsDelayedPkt	–	–	V		V	V	V	–	
cbQosTSStatsDelayed Pkt64	–	–	V		V	V	V	–	
cbQosTSStatsActive	–	–	I		I	I	I	–	This object is not supported and returns invalid data which is always zero (0) for a truthValue type.
cbQosREDClassStatsTable									The objects listed with a dash (-) are not supported.
cbQosREDECNMarkPkt Overflow	–	–	–	–	–	–	–	–	
cbQosREDECNMarkPkt	–	–	–	–	–	–	–	–	
cbQosREDECNMarkPkt64	–	–	–	–	–	–	–	–	
cbQosREDECNMarkByte Overflow	–	–	–	–	–	–	–	–	
cbQosREDECNMarkByte	–	–	–	–	–	–	–	–	
cbQosREDECNMarkByte64	–	–	–	–	–	–	–	–	
cbQosREDMeanQSizeUnits	–	–	–	–	–	–	V	–	
cbQosREDMeanQSize	–	–	–	–	–	–	V	–	
cbQosSetStatsTable									The objects listed with a dash (-) are not supported.
cbQosSetDscpPkt64	–	–	–	–	–	–	–	–	
cbQosSetPrecedencePkt64	–	–	–	–	–	–	–	–	
cbQosSetQosGroupPkt64	–	–	–	–	–	–	–	–	
cbQosSetFrDePkt64	–	–	–	–	–	–	–	–	
cbQosSetAtmClpPkt64	–	–	–	–	–	–	–	–	
cbQosSetL2CosPkt64	–	–	–	–	–	–	–	–	
cbQosSetMplsExpImposition Pkt64	–	–	–	–	–	–	–	–	
cbQosSetDiscardClassPkt64	–	–	–	–	–	–	–	–	
cbQosSetMplsExpTopMost Pkt64	–	–	–	–	–	–	–	–	
cbQosSetSrpPriorityPkt64	–	–	–	–	–	–	–	–	
cbQosSetFrFecnBecnPkt64	–	–	–	–	–	–	–	–	

Table B-4 QoS MIB Objects—Unsupported or Limited Support (continued)

MIB Tables and Objects	Policy Actions								Notes
	Band-width	Priority	Shape	Police	Queue Limit	Fair Queue	WRED	Set	
cbQosSetDscpTunnelPkt64	–	–	–	–	–	–	–	–	
cbQosSetPrecedenceTunnelPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceColorStatsTable									The objects listed with a dash (-) are not supported.
cbQosPoliceCfmColorCfmPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceCfmColorCfmByte64	–	–	–	–	–	–	–	–	
cbQosPoliceCfmColorExdPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceCfmColorExdByte64	–	–	–	–	–	–	–	–	
cbQosPoliceCfmColorVltPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceCfmColorVltByte64	–	–	–	–	–	–	–	–	
cbQosPoliceExdColorExdPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceExdColorExdByte64	–	–	–	–	–	–	–	–	
cbQosPoliceExdColorVltPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceExdColorVltByte64	–	–	–	–	–	–	–	–	
cbQosPoliceVltColorVltPkt64	–	–	–	–	–	–	–	–	
cbQosPoliceVltColorVltByte64	–	–	–	–	–	–	–	–	
cbQosPoliceCfgTable									
cbQosPoliceCfgConformColor									Not Implemented
cbQosPoliceCfgExceedColor									Not Implemented

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.

Q

QoS Quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

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

SIP SPA Interface Processor. Line card that carries the SPAs. Also referred to as MSP (Modular Services Processor and functions as a carrier card for shared port adapters)

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.

SPA Shared Port Adapter card

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