# Cisco 10000 Series Broadband MIB Specifications Guide

Release 12.2(31)SB2
May 2007

**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-2494-04a

# CONTENTS

# About This Guide

This guide describes the implementation of the Simple Network Management Protocol (SNMP) on Cisco series router configurations for Cisco IOS Release 12.2SB SNMP provides a set of commands for setting and retrieving the values of operating parameters on the router. Router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many objects that describe router components and provides information about the status of the components.

SNMP provides a set of commands for setting and retrieving the values of operating parameters on the router. Router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many objects that describe router components and provides information about the status of the components. This Preface provides an overview of this guide with the following sections:



# Revision History

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

Changes in MIB support on the Cisco 10000 Series Router occur from Cisco IOS software release to software release.

| Cisco IOS Release | Part Number | Publication Date |
|---|---|---|
| 12.2(31)SB2 | OL-4952-04a | December 2006 |

### Description of Changes

- Updated MIB Versions for 12.2SB Software Release, page 1.

- Updated the CISCO-ENTITY-ASSET-MIB with ceAssetTag constraints.
- Update ENTITY-MIB—Added UDI support and table implementation.
- Updated "Cisco 10000 Series Router MIB Categories" section on page 1.
- Added CISCO-QINQ-VLAN-MIB feature MIB.
- Added the CISCO-NETFLOW-MIB which includes SNMP access to important information available in the NetFlow Cache. This is not a replacement for the traditional NetFlow export mechanism, but a method to take a snapshot of the cache register and make it available via SNMP. This functionality is useful for security verification, discovering use of network resources, and identifying top individual contributors to network utilization.
- The CISCO-CBP-TARGET-MIB contains objects that provide a mapping of targets to which class-based features, such as QoS are applied.

  The CISCO-CBP-TARGET-MIB abstracts the knowledge of the specific types of targets from the class-based policy feature specific MIB definitions.
- Updated Appendix A with CISCO-CBP-TARGET-MIB usage information. See Appendix A, "Using CISCO-CBP-TARGET-MIB".
- CISCO-IF-EXTENSION MIB— This MIB provides two tables which provide information about interface packet statistics and interface properties respectively. These objects contain information about the interface or sub interface which is not included in the IF-MIB.
- Interface mapping improvements:
  - Improved existing CISCO-AAA-SESSION-MIB to map sessions to underlying interfaces. See Using CISCO-AAA-SESSION-MIB, page 47.
  - Improved the IF-MIB infrastructure to turn on PPP session representation and increased memory utilization with various numbers of sessions on a per interface basis.
- Added the CISCO-IP-URPF-MIB support.
- The CISCO-TAP2-MIB, page 33 has two statistics that are kept for taps:
  - Tap2StreamInterceptedPackets – the number of packets intercepted on this tap. Placed in Column 3 because this statistic can be kept anywhere from column 0 to 4 and 3 is least stressed. The column may change based on other 2.1 feature requirements but will have no impact on the feature. The counter will take a few PXF instructions (6/7) and 4k 32-bit words of XCM.
  - Tap2StreamInterceptDrops – the number of intercepted packet dropped during the intercept process. The inability to IPM_REPLAY a packet is the only drop that will be counted, therefore this counter must go into column 5. The location and bit-width of this field is uncertain at this time, but it will most likely be 4k 8-bit values in ICM or 32-bit values in XCM based on memory availability.
- MPLS-VPN-MIB, page 46 enhancement implements a new notification, VpnThreshCleared, draft-ietf-ppvpn-mpls-vpn-mib-06.txt. This notifies the network administrator that the number of routes in a VRF have fallen below the thresholds.
- Enhanced support for the OSPF-MIB to the latest RFC 1850 and adds the latest draft extensions.

| Cisco IOS Release | Part Number | Publication Date |
|---|---|---|
| 12.2(28)SB REL3 | OL-4952-03 | February 2006 |

### Description of Changes

- Added Cisco 10000 Series Router MIB categories. See Cisco 10000 Series Router MIB Categories, page 1
- Added support for the CISCO-IP-LOCAL-POOL-MIB.
- Added Table 1-1 on page 2 which lists the MIB versions that are supported in the 12.2SB REL3 and 12.3(7)XI1 software releases.
- Added support for per-Peer Received Routes in the BGP4-MIB. For detailed information, see New Features in IOS Release 12.2(28)SB at: http://lbj/push_targets1/ucdit/cc/td/doc/product/software/ios122sb/newft/122sb28/index.htm
- Added enhancements to the CISCO-FRAME-RELAY-MIB. For detailed information, see New Features in IOS Release 12.2(28)SB at: http://lbj/push_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122t/122t4/ftfrmibe.htm

| Cisco IOS Release | Part Number | Publication Date |
|---|---|---|
| 12.3(7)XI1 | OL-4952-02 | August 2004 |

### Description of Changes

- Added CISCO-IP-LOCAL-POOL-MIB, page 25.
- Enhanced snmp-server community command.See "SNMP Usage Guidelines" section on page 4 for details about the snmp-server community command use.

# Audience

This guide is intended for system and network administrators who must configure the 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 router.

# Organization

This guide contains the following chapters:

- Chapter 1, "Cisco 10000 Series Router MIB Overview," provides background information about SNMP and its implementation on the Cisco 10000 series ESR and a history revision table describing what has changed since the last software release.
- Chapter 2, "Configuring MIB Support," provides instructions for configuring SNMP management support on the router.
- Chapter 3, "MIB Specifications," describes each MIB included in the software image. Each description lists any constraints as to how the MIB is implemented on the router.
- Chapter 4, "Monitoring Notifications," describes the SNMP traps and notifications supported by the router.

- Appendix A, "Using MIBs," provides information about how to use SNMP to perform system functions such as physical entity management, alarm monitoring, bulk-file retrieval, and quality of service (QoS).
- Glossary
- Index

# Document Conventions

In this guide, command descriptions use these conventions:

| | |
|---|---|
| **boldface** font | Commands, user entry, and keywords appear in **bold**. |
| *italic* font | Arguments for which you supply values and new terms appear in *italics*. |
| [ ] | Elements in square brackets are optional. |
| { } | Elements in braces are required. |
| {x \| y \| z} | Alternative keywords are grouped in braces and separated by vertical bars. |

Examples use these conventions:

| | |
|---|---|
| `screen` font | Terminal sessions and information the system displays are in `screen` font. |
| **`bold screen`** font | Information you must enter is in **`bold screen`** font. |
| < > | Nonprinting characters such as passwords are in angle brackets. |
| [ ] | Default responses to system prompts are in square brackets. |

Notes and cautions use these conventions:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution** Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

# Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip** We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page

at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

**Note** Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

# Cisco 10000 Series Router MIB Overview

This chapter provides an overview of the Cisco 10000 series ESRenhanced MIB management feature. It includes the following sections:



## Benefits of MIB Enhancements

The Cisco 10000 series ESR enhanced MIB 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 1-5 for more information about SNMP and MIBs.

Using the enhanced management feature, you can:

- Manage and monitor Cisco 10000 resources through an SNMP-based network management system (NMS)
- Use SNMP **set** and **get** requests to access information in router MIBs
- Reduce the amount of time and system resources required to perform functions like inventory management and bulk data transfers

Other benefits include:

- A standards-based technology (SNMP) for monitoring faults and performance on the router
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3)
- Notification of faults, alarms, and conditions that might affect services
- The ability to aggregate fault and alarm information for multiple entities
- A way to access router information other than through the command line interface (CLI)

## MIB Versions for 12.2SB Software Release

The string in the table indicates the date and time that the module was most recently modified. The format is YYMMDDHHMMZ or YYYYMMDDHHMMZ

where:

- YY—last two digits of year (only years between 1900-1999)
- YYYY—last four digits of the year (any year)
- MM—month (01 through 12)
- DD—day of month (01 through 31)
- HH—hours (00 through 23)
- MM—minutes (00 through 59)
- Z—denotes GMT (the ASCII character Z)

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

Unless otherwise indicated, each MIB is included in all software images for the indicated release. In some cases, MIBs that are included in the software image are not actually supported or are only partially supported. See the individual section for each MIB for more details.

**Note** The detailed documentation in the MIB guide is only valid for MIBs that have not changed since Cisco software release 12.3(7)XI1.

Table 1-1 lists the MIB versions that are supported in the 12.3(7)XI1, 12.2SB REL3, and 12.2SB REL4 software releases.

**Note** If not specifically mentioned, the implementation is the same as the previous software release

*Table 1-1 Cisco 10000 Series Routers Supported MIB Versions*

| MIB Name | MIB Versions for 12.3(7)XI1 | MIB Versions for 12.2SB REL3 | MIB Versions for 12.2(4th)SB |
|---|---|---|---|
| ATM-MIB | 9406072245Z | 9406072245Z | 9406072245Z |
| ATM-FORUM-ADDR-REG-MIB | 9606200322Z | 9606200322Z | Not found in REL4 |
| ATM-FORUM-MIB | 9606200322Z | 9606200322Z | Not found in REL4 |
| BGP4-MIB | 9405050000Z | 9405050000Z | 9405050000Z |
| CISCO-AAA-SERVER-MIB | 2000012000000Z | 200001200000Z | 200001200000Z |
| CISCO-AAA-SESSION-MIB | 9911160000Z | 9911160000Z | 200603210000Z |
| CISCO-AAL5-MIB | 9611150000Z | 200309220000Z | 200309220000Z |
| CISCO-ATM-EXT-MIB | 9706200000Z | 200301060000Z | 200301060000Z |
| CISCO-BGP4-MIB | | | 200302240000Z |
| CISCO-BULK-FILE-MIB | 200108220000Z | 9810291700Z | 200108220000Z |
| CISCO-CDP-MIB | 9812100000Z | 9812100000Z | 200503210000Z |
| CISCO-CEF-MIB | | | 200601300000Z |

*Table 1-1 Cisco 10000 Series Routers Supported MIB Versions (continued)*

| MIB Name | MIB Versions for 12.3(7)XI1 | MIB Versions for 12.2SB REL3 | MIB Versions for 12.2(4th)SB |
|---|---|---|---|
| CISCO-CLASS-BASED-QOS-MIB | 200307240000Z | 200404120000Z | 200404120000Z |
| CISCO-CONFIG-COPY-MIB | 200205300000Z | 9701150000Z | 200403170000Z |
| CISCO-CONFIG-MAN-MIB | 9511280000Z | 9511280000Z | 9511280000Z |
| CISCO-ENTITY-ALARM-MIB | 9907062150Z | 9907062150Z | 9907062150Z |
| CISCO-ENTITY-ASSET-MIB | 9906021600Z | 200207231600Z | 200207231600Z |
| CISCO-ENTITY-EXT-MIB | 200104050000Z | 200104050000Z | 200104050000Z |
| CISCO-ENTITY-FRU-CONTROL-MIB | 200001130000Z | 200209150000Z | 200310230000Z |
| CISCO-ENTITY-PFE-MIB | 200211271600Z | 200211271600Z | 200211271600Z |
| CISCO-ENTITY-VENDOTYPE-OID-MIB | 200204051400Z | 200204051400Z | 200505050930Z |
| CISCO-ENVMON-MIB | 200108240000Z | 200207170000Z | 200207170000Z |
| CISCO-FLASH-MIB | 200301311234Z | 200301311234Z | 200301311234Z |
| CISCO-FRAME-RELAY-MIB | 200010130000Z | 200005220000Z | 200010130000Z |
| CISCO-FTP-CLIENT-MIB | 9710091700Z | 9710091700Z | 9710091700Z |
| CISCO-IETF-IP-MIB | | | 200203040000Z |
| CISCO-IETF-IP-FORWARD-MIB | | | 200201240000Z |
| CISCO-IETF-PPVPN-MPLS-VPN-MIB-MIB | | | 200304171200Z |
| CISCO-IMAGE-MIB | 9508150000Z | 9508150000Z | 9508150000Z |
| CISCO-IP-LOCAL-POOL-MIB | 200304032000Z | 200304032000Z | 200304032000Z |
| CISCO-IP-STAT-MIB | 9707180000Z | 200112202300Z | 200112202300Z |
| CISCO-IP-TAP-MIB | | | 200403110000Z |
| CISCO-IP-URPF-MIB | | | 200411120000Z |
| CISCO-IPMROUTE-MIB | 200012220000Z | 200012220000Z | 200503070000Z |
| CISCO-MEMORY-POOL-MIB | 9602120000Z | 9602120000Z | 9602120000Z |
| CISCO-NETFLOW-MIB | | | 200604200000Z |
| CISCO-OAM-MIB | 9605010000Z | 9605010000Z | 9605010000Z |
| CISCO-PIM-MIB | 200011020000Z | 200011020000Z | 200011020000Z |
| CISCO-PING-MIB | 200108280000Z | 200108280000Z | 200108280000Z |
| CISCO-PPPOE-MIB | 200102200000Z | 200102200000Z | 200102200000Z |
| CISCO-PROCESS-MIB | 200301220000Z | 200301220000Z | 200301220000Z |
| CISCO-PRODUCTS-MIB | 200204051400Z | 200204051400Z | 200505051930Z |
| CISCO-QINQ-VLAN-MIB | | | 200411290000Z |
| CISCO-RTTMON-MIB | 200305210000Z | 200401200000Z | 200501040000Z |
| CISCO-SSG-MIB | 200203250000Z | MIB Not Supported | Not found in REL4 |

*Table 1-1 Cisco 10000 Series Routers Supported MIB Versions (continued)*

| MIB Name | MIB Versions for 12.3(7)XI1 | MIB Versions for 12.2SB REL3 | MIB Versions for 12.2(4th)SB |
|---|---|---|---|
| CISCO-SYSLOG-MIB | 9508070000Z | 9508070000Z | 9508070000Z |
| CISCO-TAP2-MIB | | | 200403110000Z |
| CISCO-VPDN-MGMT-MIB | 990414000000Z | 990414000000Z | 990414000000Z |
| CISCO-VPDN-MGMT-EXT-MIB | 200207080000Z | 200207080000Z | 200207080000Z |
| DS1-MIB | 9808011830Z | 9808011830Z | 9808011830Z |
| DS3-MIB | 9808012130Z | 9808012130Z | 9808012130Z |
| ENTITY-MIB | 9912070000Z | 9912070000Z | 9912070000Z |
| ETHERLIKE-MIB | 9908240400Z | 9912070000Z | 9908240400Z |
| EVENT-MIB | 200010160000Z | 200010160000Z | 200010160000Z |
| EXPRESSION-MIB | 9802251700Z | 9802251700Z | 9802251700Z |
| IF-MIB | 9611031355Z | 9611031355Z | 9611031355Z |
| IGMP-MIB | 9712180000Z | 9712180000Z | 9712180000Z |
| IPMROUTE-MIB | 9902080000Z | 9902080000Z | Not found in REL4 |
| MPLS-LDP-MIB | 200003041200Z | 200108161200Z | 200108161200Z |
| MPLS-LSR-MIB | 200004261200Z | 200004261200Z | 200004261200Z |
| MPLS-TE-MIB | 200011211200Z | 200011211200Z | 200011211200Z |
| MPLS-VPN-MIB | 200110151200Z | 200110151200Z | 200110151200Z |
| MSDP-MIB | 9912160000Z | 9912160000Z | 9912160000Z |
| NOTIFICATION-LOG-MIB | 200011270000Z | 200011270000Z | 200011270000Z |
| PIM-MIB | 200009280000Z | 200009280000Z | 200009280000Z |
| RFC1213-MIB | 9606111939Z | 9606111939Z | 9606111939Z |
| RFC1253-MIB | 9511170836Z | 9511170836Z | Not found in REL4 |
| RFC1315-MIB | 9511170836Z | 9511170836Z | 9511170836Z |
| SNMP-FRAMEWORK-MIB | 9901190000Z | 9901190000Z | 9901190000Z |
| SNMP-MPD-MIB | 9905041636Z | 9905041636Z | 9905041636Z |
| SNMP-NOTIFICATION-MIB | 9808040000Z | 9808040000Z | 9808040000Z |
| SNMP-PROXY-MIB | 9808040000Z | 9808040000Z | 9808040000Z |
| SNMP-TARGET-MIB | 9808040000Z | 9808040000Z | 9808040000Z |
| SNMP-USM-MIB | 9901200000Z | 9901200000Z | 9901200000Z |
| SNMPv2-MIB | 9511090000Z | 9511090000Z | 9511090000Z |
| SNMP-VACM-MIB | 9901200000Z | 9901200000Z | 9901200000Z |
| SONET-MIB | 9810190000Z | 9810190000Z | 9810190000Z |
| TCP-MIB | 9411010000Z | 9411010000Z | 9411010000Z |
| UDP-MIB | 9411010000Z | 9411010000Z | 9411010000Z |

# 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:

- An 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).
- An 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).
- A Management Information Base

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or set a value in that SNMP agent.

## MIB Description

A Management Information Base (MIB) is a collection of network-management information, organized 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).
- Tabular objects—Define multiple related object instances that are grouped together in MIB tables (for example, ifTable in the IF-MIB defines the interface entities on the router).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—This 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—This function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

# SNMP Traps

An SNMP agent can send messages to 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, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host. SNMP notifications can be sent as either *traps* or *informs*. See Chapter 4, "Monitoring Notifications," for information about traps.

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

# SNMP Versions

Cisco IOS software supports the following versions of SNMP:

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

## SNMPv1 and SNMPv2c

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

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

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

### SNMPv3

SNMPv3 provides 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 which security mechanism is employed when handling an SNMP packet.

### SNMP Security Models and Levels

Table 1-2 describes the security models and levels provided by the different SNMP versions.

*Table 1-2 SNMP Security Models and Levels*

| Model | Level | Authentication | Encryption | Description |
|---|---|---|---|---|
| v1 | noAuthNoPriv | Community string | No | Uses match on community string for authentication. |
| v2c | noAuthNoPriv | Community string | No | Uses match on community string for authentication. |
| v3 | noAuthNoPriv | User name | No | Uses match on user name for authentication. |
| | authNoPriv | MD5 or SHA | No | Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. |
| | authPriv | MD5 or SHA | DES | Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. Also provides DES 56-bit encryption based on CBC-DES (DES-56) standard. |

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

## Requests For Comments

MIB modules are written in the SNMP MIB module language, and are typically defined in Request For Comments (RFC) documents submitted to the Internet Engineering Task Force (IETF). RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole. Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (http://www.isoc.org and http://www.ietf.org).

We provide private MIB extensions with each Cisco system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation.

## Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices. Top-level MIB OIDs are assigned by standards organizations such as ISO and ITU, while lower-level OIDs are assigned by associated organizations such as the 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*-MIB represents the *xyz*-MIB whose location in the MIB hierarchy is as follows. Note that the numbers in parentheses are included only to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).*nn*-MIB

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.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/

# Related Information and Useful Links

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

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

## TAC Information and FAQs

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

- http://www.cisco.com/warp/public/477/SNMP/index.html is the Cisco TAC page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.

## SNMP Configuration Information

The following URLs provide information about configuring SNMP:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/cfun_vcg.htm provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/index.htm provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.

CHAPTER 2

# Configuring MIB Support

This chapter describes how to configure SNMP and MIB support for the Cisco 10000 series ESR. It includes the following sections:



## Determining MIB Support for Cisco IOS Releases

Follow these steps to determine which MIBs are included in the Cisco IOS release running on the router:

**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 10000** to display a list of MIBs supported on the router.

**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 router:



### Considerations for Working with MIBs

While working with MIBs, consider the following:

- Mismatches on datatype definitions might cause compiler errors or warning messages. For example, the OLD-CISCO-CPU-MIB, OLD-CISCO-MEMORY-MIB, and OLD-CISCO-SYSTEM-MIB each define the following OID differently:

```
OLD-CISCO-CPU-MIB.my
     lcpu    OBJECT IDENTIFIER ::= {local 1 }

OLD-CISCO-MEMORY-MIB.my
     lenv    OBJECT IDENTIFIER ::= {local 1 }
```

To eliminate MIB compiler errors or warning messages for mismatched definitions, edit one of the MIB definitions to match the other. Other types of mismatches include:

```
MIB A
Datatype1 ::= INTEGER(0...100)
Datatype2 ::= INTEGER(1...50)

MIB B
Datatype1 ::= DisplayString
Datatype2 ::= OCTET STRING (SIZE(0...255))
```

- 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:

  SNMPv2-SMI.my
  SNMPv2-TC.my
  SNMPv2-MIB.my
  RFC1213-MIB.my
  IF-MIB.my
  CISCO-SMI.my
  CISCO-PRODUCTS-MIB.my
  CISCO-TC.my

- For information about trap definitions, alternative size definitions, and null OIDs, go to the following URL:

  ftp://ftp.cisco.com/pub/mibs/app_notes/mib-compilers

- For listings of OIDs assigned to MIB objects, go to the following URL:

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

- For additional information about downloading and compiling MIBs, go to the bottom of the page at the following URL:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.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 previous section ("Considerations for Working with MIBs").

**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.atmforum.com

## Compiling MIBs

If you plan to integrate the Cisco 10000 series ESR with an SNMP-based management application, you must also compile the MIBs for that platform. For example, if you are running HP OpenView on the UNIX operating system, you must compile the router MIBs with the HP OpenView network management system (NMS). For instructions, see the NMS documentation.

# Cisco SNMP Support

The following sections provide information about SNMP support for the Cisco 10000 series ESR:



## Enabling SNMP Support

The SNMP agent is disabled by default. The following procedure summarizes how to configure the Cisco 10000 series ESR for SNMP support. Note that these basic configuration commands are issued for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups.

**Step 1** Set up your basic SNMP configuration through the command line interface (CLI). (For command and setup information, see the list of documents that follows this procedure.)

**Step 2** Define SNMP 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
```

**Step 3** 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 4** See the "Enabling Notifications" section on page 4-2 for information on how to enable traps.

### Configuration Examples

This section lists configuration examples showing how to enable the SNMP agent.

```
Router# configure terminal
Router(config)# snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string public.

```
Router(config)# snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the command access community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro 4
```

# Verifying SNMP Support

To verify that the SNMP agent has been enabled on the router, display the running configuration and look for SNMP information. Enter the following command:

```
Router(config)# show running-configuration
...
...
snmp-server community public RO
```

If you see any snmp-server statements, then SNMP is enabled on the router.

# SNMP Usage Guidelines

This section describes the **snmp-server community** command. To configure read-only or read/write Simple Network Management Protocol (SNMP) community strings, use the **snmp-server community** command in the global configuration mode.

To change the community string to its default value, use the **no** form of this command:

```
snmp-server community string [view view-name] [ro | rw] [number]
no snmp-server community string
```

Where:

- **community string** is a string of 1 to 32 alphanumeric characters. The community string acts like a password and permits access to the SNMP protocol.
- **view view-name** is the nme of a previously defined view (optional). The view defines the objects available to the community.
- **ro** configures read-only access
- **rw** configures read/write access.
- **number** is the integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMPv1 agent.

## Important Notes about SNMP-Server Community Command

The following is a list of SNMP usage information:

- The default value of the read/write parameter is read-only (**ro**). The default value of the read-only community string is **public**, and the default value of the read/write community string is **private**.
- The **no snmp-server** command disables both versions of SNMP (SNMPv1 and SNMPv2).
- The first snmp-server command that you enter enables both versions of SNMP.

**Note** All other commands used with this feature are documented in the Cisco command reference publications. Related commands are **snmp-server-enable traps** and **snmp-server host**.

### Read/Write Community String Examples

- In this example, the read/write community string is set to newstring:

```
Router(config)# snmp-server community newstring rw
```

- The string comaccess is assigned to SNMPv1, allowing read-only access. IP access list 4 is enabled to use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

- The string mgr is assigned to SNMPv1, allowing read/write access to the objects in the restricted view:

```
Router(config)# snmp-server community mgr view restricted rw
```

- The community comaccess is removed:

```
Router(config)# no snmp-server community comaccess
```

- Both versions of SNMP are disabled:

```
Router(config)# no snmp-server
```

## SNMP Related Information

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

- *Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide*, available at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/cfun_vcg.htm

- *Cisco IOS Release 12.3 Configuration Fundamentals Command Reference*, available at the the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/fun_r/index.htm

CHAPTER 3

# MIB Specifications

This chapter describes each Management Information Base (MIB) on the Cisco 10000 series ESR. Each description lists any constraints on how the MIB is implemented on the router. Unless noted otherwise, the Cisco 10000 Series router implementation of a MIB follows the standard. For detailed MIB descriptions, see the MIB.

**Note** For information about how to avoid performance problems when you use SNMP to poll the router for routing table entries, see the "Cisco SNMP Support" section on page 2-3. To determine which MIBs are included in other releases, see the "Determining MIB Support for Cisco IOS Releases" section on page 2-1.

## Cisco 10000 Series Router MIB Categories

Not all MIBs included in a Cisco IOS release are fully supported by the 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.

The following tables list the categories of MIBs in the c10k Image for Cisco IOS Release 12.2SB REL4. for configurations on the Cisco 10000 series ESR:

- Supported and tested for Cisco10000 series router MIBs—The MIB exists in the image, the code is implemented, and the MIBs have been tested.
- Supported and not tested for Cisco 10000 series router MIBs—The MIB exists in the image, the code is implemented, but we have not verified if it is working properly. In other words, the user may get something if they query the MIB. However, the information may be correct or incorrect because the MIB has not been tested.
- Unsupported and not tested MIBs (no level of support or testing on the Cisco 10000 series router)—The MIB maybe posted in CCO, but it is not present in the image and can not be queried.

**Note** The RFC versions are listed to show the MIB versions we support.

# Supported and Tested MIBs

Table 3-1 lists the MIBs included in Cisco IOS EFT software release 12.2SB REL4 that are *supported* and *tested* for configurations on the Cisco 10000 series ESR. To determine which MIBs are included in other releases, see the "Determining MIB Support for Cisco IOS Releases" section on page 2-1.

***Table 3-1 Supported and Tested Cisco 10000 Series Router MIBs in the c10k Image***

| | |
|---|---|
| ATM-MIB | CISCO-IP-STAT-MIB |
| BGP4-MIB | CISCO-IP-TAB-MIB |
| CISCO-IF-EXTENSION-MIB | CISCO-NETFLOW-MIB |
| CISCO-CBP-TARGET-MIB | CISCO-OAM-MIB |
| CISCO-CEF-MIB | CISCO-PPPOE-MIB |
| CISCO-AAA-SERVER-MIB | CISCO-PROCESS-MIB |
| CISCO-AAA-SESSION-MIB | CISCO-RF-MIB |
| CISCO-AAL5-MIB | CISCO-RTTMON-MIB |
| CISCO-ATM-EXT-MIB | CISCO-QUEUE-MIB |
| CISCO-BGP4-MIB | CISCO-SSG-MIB |
| CISCO-BULK-FILE-MIB | CISCO-SYSLOG-MIB |
| CISCO-CLASS-BASED-QOS-MIB | DS1-MIB |
| CISCO-CONFIG-COPY-MIB | DS3-MIB |
| CISCO-CONFIG-MAN-MIB | ENTITY-MIB |
| CISCO-ENTITY-ALARM-MIB | ETHERLIKE-MIB |
| CISCO-ENTITY-ASSET-MIB | IF-MIB |
| CISCO-ENTITY-EXT-MIB | IP-MIB |
| CISCO-ENTITY-FRU-CONTROL-MIB | NOTIFICATION-LOG-MIB |
| CISCO-ENTITY-PFE-MIB | OSPF-MIB |
| CISCO-ENTITY-VENDORTYPE-OID-MIB | CISCO-QINQ-VLAN-MIB |
| CISCO-ENVMON-MIB | RFC1315-MIB |
| CISCO-FLASH-MIB | RMON-MIB |
| CISCO-FRAME-RELAY-MIB | RSVP-MIB |
| CISCO-FTP-CLIENT-MIB | SNMP-NOTIFICATION-MIB |
| CISCO-IP-LOCAL-POOL-MIB | SONET-MIB |
| CISCO-IPMROUTE-MIB | -- |
| CISCO-IP-URPF-MIB | -- |

# Supoorted and Not Tested MIBs

Table 3-2 lists the MIBs included in Cisco IOS EFT software release 12.2SB REL4 that are *supported* but *not tested* for configurations on the Cisco 10000 series ESR router.

*Table 3-2 Supported and Not Tested Cisco 10000 Series Router MIBs in the c10k Image*

| | |
|---|---|
| CISCO-ACCESS-ENVMON-MIB | MPLS-LDP-MIB (version 8) |
| ATM-FORUM-ADDR-REG-MIB | MPLS-LSR-MIB |
| ATM-FORUM-MIB | MPLS-TE-MIB |
| CISCO-CDP-MIB | MPLS-VPN-MIB |
| CISCO-TCP-MIB | MSDP-MIB |
| CISCO-HSRP-MIB | OLD-CISCO-CHASSIS-MIB (deprecated MIB) |
| CISCO-HSRP-EXT-MIB | OLD-CISCO-CPU-MIB (deprecated MIB) |
| CISCO-IETF-ATM2-PVCTRAP-MIB | OLD-CISCO-INTERFACES-MIB (deprecated MIB) |
| CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN | OLD-CISCO-IP-MIB (deprecated MIB) |
| CISCO-IMAGE-MIB | OLD-CISCO-MEMORY-MIB (deprecated MIB) |
| CISCO-IPMROUTE-MIB | OLD-CISCO-SYSTEM-MIB (deprecated MIB) |
| CISCO-IP-LOCAL-POOL-MIB | OLD-CISCO-TCP-MIB (deprecated MIB) |
| CISCO-MEMORY-POOL-MIB | OLD-CISCO-TS-MIB (deprecated MIB) |
| CISCO-PIM-MIB | PIM-MIB |
| CISCO-PING-MIB | RFC1213-MIB |
| CISCO-SNAPSHOT-MIB | RFC1253-MIB |
| INT-SERV-GUARANTEED-MIB | RS-232-MIB |
| CISCO-VPDN-MGMT-MIB | SNMP-FRAMEWORK-MIB |
| CISCO-VPDN-MGMT-EXT-MIB | SNMP-MPD-MIB |
| EVENT-MIB | SNMP-PROXY-MIB |
| EXPRESSION-MIB | SNMP-TARGET-MIB |
| IGMP-MIB | SNMP-USM-MIB |
| IPMROUTE-MIB | SNMPv2-MIB |
| IP-FORWARD-MIB | SNMP-VACM-MIB |
| INT-SERV-MIB | TCP-MIB |
| INT-SERV-GUARANTEED-MIB | UDP-MIB |

# Unsupported and Not Tested MIBs

Table 3-3 lists MIBs that are *unsupported or not tested*.

*Table 3-3 Unsupported and Not Tested Cisco 10000 Series Router MIBs in the c10k Image*

| | |
|---|---|
| CISCO-PRODUCTS-MIB | CISCO-VOICE-COMMON-DIAL-CONTROL-MIB |
| CISCO-ACCESS-ENVMON-MIB | CISCO-VOICE-DIAL-CONTROL-MIB |
| CISCO-ALPS-MIB | CISCO-VOICE-IF-MIB |
| CISCO-TAP2-MIB | CISCO-VINES-MIB |

**Note** The remaining sections of this chapter list MIBs that are in the Cisco 10000 series router image in addition to any constraints for a MIB. Any MIB table or object not listed in a table is implemented as defined in the MIB. However, support may be unverified or the MIB may not be supported.

# ATM-FORUM-ADDR-REG-MIB

The ATM-FORUM-ADDR-REG-MIB contains information about ATM user-network interface (UNI) addresses and ports. The MIB also contains ATM address registration administration information.

There are no constraints on this MIB.

# ATM-FORUM-MIB

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

There are no constraints on this MIB.

# ATM-MIB

The ATM-MIB contains the ATM and ATM adaptation layer 5 (AAL5) objects used to manage ATM interfaces, virtual links, cross connects, and AAL5 entities and connections.

## MIB Constraints

Table 3-4 lists the constraints that the router places on objects in the ATM-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-4 ATM-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **atmInterfaceConfTable** | Read-only. |
| • atmInterfaceMaxVpcs | Always 0. Virtual paths are not applicable. |
| • atmInterfaceConfVpcs | Always 0. Virtual paths are not applicable. |
| • atmInterfaceAddressType | Always private(1). |
| • atmInterfaceAdminAddress | Always NULL. |
| **atmInterfaceDs3PlcpTable** | Not used in Cisco 10000 configurations. |
| **atmInterfaceTCTable** | Not implemented. |
| **atmTrafficDescrParamTable** | Read-only. |
| **atmVplTable** | Read-only. |
| **atmVclTable** | Read-only. |
| **atmVpCrossConnectTable** | Not used in Cisco 10000 configurations. |

*Table 3-4 ATM-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| **atmVcCrossConnectTable** | Not used in Cisco 10000 configurations. |
| **aal5VccTable** | Not implemented. |

# BGP4-MIB

The 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
- Ability to query total number of routes received/neigh via SNMP
- Support for BGP FSM transition trap
- BGP Prefix threshold trap
- MIB object for BGP prefix threshold

There are no constraints on this MIB.

# CISCO-CEF-MIB

The CISCO-CEF-MIB (Cisco Express Forwarding) 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.

**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-AAA-SERVER-MIB

The CISCO-AAA-SERVER-MIB contains information about authentication, authorization, and accounting (AAA) servers within the router and external to the router. The 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 objects in the CISCO-AAA-SERVER-MIB. For detailed definitions of MIB objects, see the 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 is 1646. |
| • casKey | Read-only. This value always shown as " " (null string) for security reasons. |
| • casConfigRowStatus | Read-only. |
| **casStatisticsTable** | |
| • casAuthorRequests<br>• casAuthorRequestTimeouts<br>• casAuthorUnexpectedResponses<br>• casAuthorServerErrorResponses<br>• casAuthorIncorrectResponses<br>• casAuthorResponseTime<br>• casAuthorTransactionSuccesses<br>• casAuthorTransactionFailures | For RADIUS servers, these values are always 0. (RADIUS does not make authorization requests.)<br>Only TACACS+ servers can have nonzero values. |

# CISCO-AAA-SESSION-MIB

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

## MIB Constraints

Table 3-6 lists the constraints that the router places on objects in the CISCO-AAA-SESSION-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-6 CISCO-AAA-SESSION-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **casnActiveTable** | |
| • casnDisconnect | To use this object to disconnect from an AAA server through SNMP, you must have enabled the functionality through the CLI command **aaa session-mib disconnect**. |
| • casnNasPort | Read-only. |
| • casnVaiIfIndex | Read-only. |

**Note** These objects casnNasPort and casnVaiIfIndex are supported for PPPoE (support should be available for this release) and PPPoA sessions in the CISCO-AAA-SESSION-MIB.

# CISCO-AAL5-MIB

The CISCO-AAL5-MIB contains performance statistics for ATM adaptation layer 5 (AAL5) virtual channel connections (VCCs). This MIB provides statistics not found in the aal5VccTable in RFC 1695 (for example, packets and octets received and transmitted on the VCC).

There are no constraints on this MIB.

# CISCO-ACCESS-ENVMON-MIB

The CISCO-ACCESS-ENVMON-MIB indicates the reason for a power supply failure, which is information not found in the ciscoEnvMonSupplyStatusTable in the CISCO-ENVMON-MIB. The CISCO-ACCESS-ENVMON-MIB also defines temperature and voltage notifications to replace those in CISCO-ENVMON-MIB. This MIB is deprecated.

# CISCO-ATM-EXT-MIB

The CISCO-ATM-EXT-MIB contains extensions to the Cisco ATM module that are used to manage ATM entities. It provides additional AAL5 performance statistics for a virtual channel connection (VCC) on an ATM interface. There are no constraints on this MIB.

# 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

Table 3-7 lists the constraints that the router places on objects in the CISCO-CBP-TARGET-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-7 CISCO-CBP-TARGET-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **CbpTargetTable** | |
| • ccbptTargetType | Values are:<br>• genIf(1<br>• atmPvc(2)<br>• frDlci(3)<br>• controlPlane(4) |
| • ccbptTargetDir | Values are:<br>• input(2)<br>• 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 active(1) |
| • ccbptPolicyMap | Contains the OID for a cbQosPolicyMapName instance |
| • ccbptPolicyInstance | Contains the OID for a cbQosIfType instance |

# CISCO-BGP4-MIB

The CISCO-BGP4-MIB contains Cisco defined extensions to the BGP4-MIB.

There are no constraints on this MIB.

# 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 3-8 lists the constraints that the router places on objects in the CISCO-BULK-FILE-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-8 CISCO-BULK-FILE-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **cbfDefineFileTable** | |
| • cbfDefineFileStorage | Only ephemeral(1) supported. |
| • cbfDefineFileFormat | Data format standardBER(1) not supported. |

# CISCO-CDP-MIB

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

There are no constraints on this MIB.

# CISCO-CLASS-BASED-QOS-MIB

The Class-Based Quality of Service Management Information Base (CBQoS- MIB) provides access to quality of service (QoS) configuration information and statistics. The CBQoS-MIB allows service providers to monitor their QoS offerings. This MIB gives QoS configuration done in the router such as ClassMap, PolicyMap, Match Statements and Feature Actions configuration parameters.

The MIB contains counter objects which provides statistic information such as the number of packets traversed conforming to a policing feature. The MIB uses several indexes to identify QoS features and to distinguish among instances of those features. The MIB provides information about marking and policing done using IP precedence and Differentiated Services Code Point (DSCP).

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

- cbQosREDValue—The IP precedence or IP differentiated services code point (DSCP) of a Weighted Random Early Detection (WRED) action. It is used as the index for configuration information and statistics for each RED class. The IP Precedence or DSCP of a WRED action can be displayed.
- cbQosPolicyIndex—Identifies a service policy attached to a logical interface.
- cbQosObjectsIndex—Identifies each QoS feature on the Cisco 10000 series ESR.
- cbQosConfigIndex—Identifies a type of QoS configuration. This index is shared by QoS objects that have identical configurations.

The indexes cbQosPolicyIndex and cbQosObjectsIndex are assigned by the system to uniquely identify each instance of a QoS feature. These indexes are never reused between router reboots, even if the QoS configuration changes.

QoS information is stored in:

- Configuration objects—Might have multiple identical instances. Multiple instances of the same QoS feature share a single configuration object, which is identified by cbQosConfigIndex.
- Statistics objects—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.

For detailed information about QoS, see its feature description at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kftmap/map.htm

# MIB Constraints

Table 3-9 lists the constraints that the router places on objects in the CISCO-CLASS-BASED-QOS-MIB. For detailed definitions of MIB objects, see the MIB.

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

| MIB Object | Notes |
|---|---|
| **cbQosInterfacePolicyTable** | |
| • cbQosIFPolicyIndex | Not supported. Always 0. |
| **cbQosFrameRelayPolicyTable** | |
| • cbQosFRPolicyIndex | Not supported. Always 0. |
| **cbQosATMPVCPolicyTable** | |
| • cbQosATMPolicyIndex | Not supported. Always 0. |
| **cbQosQueueingCfgTable** | |
| • cbQosQueueingCfgFlowEnabled | Not supported. Always false(2). |
| • cbQosQueueingCfgIndividualQSize | Not supported. Always 0. |
| • cbQosQueueingCfgDynamicQNumber | Not supported. Always 0. |
| • cbQosQueueingCfgPrioBurstSize | Not supported. Always 0. |
| **cbQosPoliceCfgTable** | |
| • cbQosPoliceCfgViolateAction | Not supported. Always 0. |
| • cbQosPoliceCfgViolateSetValue | Not supported. Always 0. |
| **cbQosTSCfgTable** | |
| • cbQosTSCfgBurstSize | Not supported. Always 0. |
| • cbQosTSCfgExtBurstSize | Not supported. Always 0. |
| • cbQosTSCfgAdaptiveEnabled | Not supported. Always false(2). |
| • cbQosTSCfgAdaptiveRate | Not supported. Always 0. |
| • cbQosTSCfgLimitType | Not supported. Always average(1). |
| **cbQosCMStatsTable** | |
| • cbQosCMDropByte64<br>• cbQosCMDropByteOverflow<br>• cbQosCMDropByte | Only police drops are monitored, no queueing drops. |
| **cbQosPoliceStatsTable** | |

*Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • cbQosPoliceViolatedPkt64<br>• cbQosPoliceViolatedPktOverflow<br>• cbQosPoliceViolatedPkt<br>• cbQosPoliceViolatedByte64<br>• cbQosPoliceViolatedByteOverflow<br>• cbQosPoliceViolatedByte<br>• cbQosPoliceConformedBitRate<br>• cbQosPoliceExceededBitRate<br>• cbQosPoliceViolatedBitRate | These objects not supported. Always 0. |
| **cbQosQueueingStatsTable** | |
| • cbQosQueueingDiscardByte64<br>• cbQosQueueingDiscardByteOverflow<br>• cbQosQueueingDiscardByte | These objects not supported. Always 0. |
| **cbQosTSStatsTable** | |
| • cbQosTSStatsDelayedByteOverflow<br>• cbQosTSStatsDelayedByte<br>• cbQosTSStatsDelayedByte64<br>• cbQosTSStatsDelayedPktOverflow<br>• cbQosTSStatsDelayedPkt<br>• cbQosTSStatsDelayedPkt64<br>• cbQosTSStatsDropByteOverflow<br>• cbQosTSStatsDropByte<br>• cbQosTSStatsDropByte64 | These objects not supported. Always 0. |
| • cbQosTSStatsActive | Not dynamic. If traffic shaping is configured, cbQosTSStatsActive is true(1); otherwise, it is false(2). |
| **cbQosREDClassStatsTable** | |
| • cbQosREDRandomDropPktOverflow<br>• cbQosREDRandomDropPkt<br>• cbQosREDRandomDropPkt64 | Counts are recorded per class, not cbQosREDValue (IP precedence or DSCP). All counters with the same cbQosREDValue contain the same count. |
| • cbQosREDRandomDropByteOverflow<br>• cbQosREDRandomDropByte<br>• cbQosREDRandomDropByte64 | These objects not supported. Always 0. |

*Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • cbQosREDTailDropPktOverflow<br>• cbQosREDTailDropPkt<br>• cbQosREDTailDropPkt64 | Counts are recorded per class, not cbQosREDValue (IP precedence or DSCP). All counters with the same cbQosREDValue contain the same count. |
| • cbQosREDTailDropByteOverflow<br>• cbQosREDTailDropByte<br>• cbQosREDTailDropByte64 | These objects not supported. Always 0. |
| • cbQosREDTransmitPktOverflow<br>• cbQosREDTransmitPkt<br>• cbQosREDTransmitPkt64<br>• cbQosREDTransmitByteOverflow<br>• cbQosREDTransmitByte<br>• cbQosREDTransmitByte64 | Counts are recorded per class, not cbQosREDValue (IP precedence or DSCP). All counters with the same cbQosREDValue contain the same count. |

# 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
- Copy the running config to the startup config and startup to running
- Copy the startup or running config files to and from a local Cisco IOS file system

## MIB Constraints

You can use a Trivial File Transfer Protocol (TFTP) server to copy configuration files to and from the network.

Table 3-10 lists the constraints that the router places on objects in the CISCO-CONFIG-COPY-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-10 CISCO-CONFIG-COPY-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **ccCopyTable** | |
| • ccCopyProtocol | File Transfer Protocol, ftp(2), and remote copy procotol, rcp(3), are not supported. Only Trivial File Transfer Protocol, tftp(1), is valid. |
| • ccCopySourceFileType<br>• ccCopyDestFileType | The values iosFile(2) and terminal(5) are not supported for source and destination file types. |

*Table 3-10 CISCO-CONFIG-COPY-MIB Constraints*

| MIB Object | Notes |
|---|---|
| • ccCopyUserName | Not supported. Only valid when FTP and RCP are supported. |
| • ccCopyUserPassword | Not supported. Only valid when FTP and RCP are supported. |

# 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.

There are no constraints on this MIB.

# CISCO-ENTITY-ALARM-MIB

The CISCO-ENTITY-ALARM-MIB enables the router to monitor alarms generated by system components, such as the chassis, slots, modules, power supplies, fans, and module ports. For information about alarms and corrective actions, see the *Cisco 10000 Series Router Troubleshooting Guide* (which is listed below the Cisco 10000 Series Router Technical Reference documentation).

For a component's alarms to be monitored, the component must be defined by a row in the entPhysicalTable of the ENTITY-MIB.

**Note** The CISCO-ENTITY-ALARM-MIB monitors the alarms of physical entities only.

## MIB Constraints

Table 3-11 lists the constraints that the router places on objects in the CISCO-ENTITY-ALARM-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-11 CISCO-ENTITY-ALARM-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **ceAlarmDescrTable** | |
| • ceAlarmDescrSeverity | Read-only. |
| ceAlarmFilterProfileIndexNext | Not implemented. |
| **ceAlarmFilterProfileTable** | Not implemented. |

# CISCO-ENTITY-ASSET-MIB

The CISCO-ENTITY-ASSET-MIB provides asset tracking information for the physical components in the ENTITY-MIB entPhysicalTable.

The ceAssetTable contains an entry (ceAssetEntry) for each physical component on the router. Each entry provides information about the component, such as its orderable part number, serial number, hardware revision, manufacturing assembly number and 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 CISCO-ENTITY-ASSET-MIB accesses the component's ID PROM information. However, if no ID PROM information is available, the MIB returns the values listed in Table 3-13 on page 3-14.

# MIB Constraints

Table 3-12 lists the constraints that the router places on objects in the CISCO-ENTITY-ASSET-MIB. For detailed definitions of MIB objects, see the MIB.

***Table 3-12 CISCO-ENTITY-ASSET-MIB Constraints***

| MIB Object | Notes |
|---|---|
| **ceAssetTable** | |
| • ceAssetAlias | Not implemented. |
| • ceAssetTag | Implemented only for PRE and Line Cards which have EEPROM information for Asset ID. |

Table 3-13 on page 3-14 lists the values that SNMP returns for ceAssetEntry objects if no ID PROM information exists for a component. The definition of ceAssetEntry is as follows:

```
CeAssetEntry ::= SEQUENCE {
    ceAssetOEMString              SnmpAdminString,
    ceAssetSerialNumber           SnmpAdminString,
    ceAssetOrderablePartNumber    SnmpAdminString,
    ceAssetHardwareRevision       SnmpAdminString,
    ceAssetMfgAssyNumber          SnmpAdminString,
    ceAssetMfgAssyRevision        SnmpAdminString,
    ceAssetFirmwareID             SnmpAdminString,
    ceAssetFirmwareRevision       SnmpAdminString,
    ceAssetSoftwareID             SnmpAdminString,
    ceAssetSoftwareRevision       SnmpAdminString,
    ceAssetCLEI                   SnmpAdminString,
    ceAssetTag                    SnmpAdminString,
    ceAssetIsFRU                  TruthValue
}
```

Not all ceAssetEntry objects are used by all router components, and ceAssetAlias is not implemented for the Cisco 10000 series ESR.

***Table 3-13 Cisco 10000 ceAssetEntry Values***

| MIB Object | ceAssetEntry Value | Type |
|---|---|---|
| **Chassis** | | |
| ceAssetOEMString | Cisco Systems, Inc. | — |
| ceAssetOrderablePartNumber | 10008 | Cisco 10008 chassis |

*Table 3-13 Cisco 10000 ceAssetEntry Values (continued)*

| MIB Object | ceAssetEntry Value | Type |
|---|---|---|
| ceAssetIsFRU | true | — |
| All other ceAssetEntry object | " " (null string) | — |
| **PREs—Performance Routing Engine/Forwarding Processor** | | |
| ceAssetOEMString | Cisco Systems, Inc. | — |
| ceAssetOrderablePartNumber | PRE2<br>" " (null string) | Performance Routing Engine<br>Forwarding Processor |
| ceAssetFirmwareID | The FP software ID<br>" " (null string) | PRE<br>FP |
| ceAssetFirmwareRevision | The FP firmware revision<br>" " (null string) | PRE<br>FP |
| ceAssetSoftwareID | The Cisco IOS image ID<br>The image ID of FP microcode | PRE<br>FP |
| ceAssetSoftwareRevision | The Cisco IOS image version<br>The image version of FP microcode | PRE<br>FP |
| ceAssetCLEI | " " | — |
| ceAssetTag | " " | — |
| ceAssetIsFRU | true<br>false | PRE<br>FP |
| All other ceAssetEntry objects | " " | — |
| **Power Supplies—AC/DC** | | |
| ceAssetOEMString | Cisco Systems, Inc. | — |
| ceAssetOrderablePartNumber | PWR-AC<br>PWR-DC | AC power supply<br>DC power supply |
| ceAssetIsFRU | true | — |
| All other ceAssetEntry objects | " " | — |
| **Flash Cards—48 Mbyte/128 Mbyte** | | |

*Table 3-13 Cisco 10000 ceAssetEntry Values (continued)*

| MIB Object | ceAssetEntry Value | Type |
|---|---|---|
| ceAssetOrderablePartNumber | PRD-MEM-FD48<br>PRD-MEM-FD128 | 48 Mbyte flash card<br>128 Mbyte flash card |
| ceAssetIsFRU | true | — |
| All other ceAssetEntry objects | " " | — |
| **Fan Tray Assemblies** | | |
| ceAssetOEMString | Cisco Systems, Inc. | — |
| ceAssetOrderablePartNumber | BLOWER | Cisco 10008 chassis |
| ceAssetIsFRU | true | — |
| All other ceAssetEntry objects | " " | — |
| **Line Cards** | | |
| ceAssetOEMString | Cisco Systems, Inc. | — |
| ceAssetOrderablePartNumber | 1GE | Gigabit Ethernet (1-port) line card |
| | HH-1GE | Gigabit Ethernet (1-port) half-height line card |
| | HH-8FE-TX | Fast Ethernet (8-port) half-height line card |
| | 24CT1/E1 | Channelized E1/T1 (24-port) line card |
| | 6CT3 | Channelized T3 (6-port) line card |
| | 8E3/DS3 | E3/DS3 (8-port) line card |
| | 8E3/DS3ATM | E3/DS3 ATM (8-port) line card |
| | 6OC3/P-SMI | OC-3 POS (6-port) line card |
| | 1OC12/P-SMI | OC-12 POS (1-port) line card |
| | 1OC48/P | OC-48 (1-port) line card |
| | 4OC3ATM-SM | OC-3 ATM (4-port) line card |
| | OC12ATM-SM | OC-12/STM-4 ATM (1-port) line card |
| | 4OC3-CHSTM1 | Channelized OC-3/STM-1 (4-port) line card |
| | 1COC12-SMI | Channelized OC-12 (1-port) line card |

*Table 3-13 Cisco 10000 ceAssetEntry Values (continued)*

| MIB Object | ceAssetEntry Value | Type |
|---|---|---|
| ceAssetSoftwareID | 1GE-LCDOS | Gigabit Ethernet line-card software |
| | HH-1GE-LCDOS | Gigabit Ethernet half-height line card software |
| | HH-8FE-TX-LCDOS | Fast Ethernet half-height line card software |
| | 24CT1/E1-LCDOS | Channelized E1/T1 line-card software |
| | 6CT3-LCDOS | Channelized T3 line-card software |
| | 8E3/DS3-LCDOS | E3/DS3 line-card software |
| | 8E3/DS3ATM-LCDOS | E3/DS3 ATM line-card software |
| | 6OC3/P-SMI-LCDOS | OC-3 POS line-card software |
| | 1OC12/P-SMI-LCDOS | OC-12 POS line-card software |
| | 1OC48/P-LCDOS | OC-48 POS line-card software |
| | 4OC3ATM-LCDOS | OC-3 ATM line-card software |
| | 1OC12ATM-LCDOS | OC-12/STM-4 ATM line-card software |
| | 4OC3-LCDOS | Channelized OC-3/STM-1 line-card software |
| | 1COC12-LCDOS | Channelized OC-12 line-card software |
| ceAssetSoftwareRevision | The current line card software revision | — |
| ceAssetIsFRU | true | — |
| All other ceAssetEntry objects | " " | — |

# CISCO-ENTITY-EXT-MIB

The CISCO-ENTITY-EXT-MIB contains extensions for active and standby Performance Routing Engines (PREs) listed in the ENTITY-MIB entPhysicalTable. These extensions provide information such as RAM and NVRAM sizes, configuration register settings, and bootload image name for each PRE.

## MIB Constraints

Table 3-14 lists the constraints that the router places on objects in the CISCO-ENTITY-EXT-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-14 CISCO-ENTITY-EXT-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **ceExtPhysicalProcessorTable** | Supports active and standby PREs only. Line cards with a processor are currently not supported. |

*Table 3-14 CISCO-ENTITY-EXT-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| **ceExtConfigRegTable** | |
| • ceExtConfigRegNext | Read-only. |

# CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB contains objects to configure and monitor the status of field replaceable units (FRUs) on the Cisco 10000 series ESR. An FRU is a hardware component (such as a line card, power supply, or fan) that can be replaced on site.

## MIB Constraints

Table 3-15 lists the constraints that the router places on objects in the CISCO-ENTITY-FRU-CONTROL-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-15 CISCO-ENTITY-FRU-CONTROL-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **cefcFRUPowerSupplyGroupTable** | Not implemented. |
| **cefcFRUPowerStatusTable** | Not implemented. |
| cefcMaxDefaultInLinePower | Not implemented. |
| **cefcModuleTable (line card entities)** | |
| • cefcModuleAdminStatus | Supported values for SET operation:<br>enabled(1)<br>disabled(2)<br>reset(3)<br>When this object is set to enabled(1), a reset(3) changes the line card operational state to the boot state. When set to disabled(2), a reset changes the line card operational state to the boot state and returns the value enabled(1). |
| • cefcModuleOperStatus | Supported values:<br>ok(2)<br>disabled(3)<br>boot(5)<br>missing(8)<br>If a line card is provisioned for a slot but it is not present in the slot, the card's operational state is missing(8). |

*Table 3-15 CISCO-ENTITY-FRU-CONTROL-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • cefcModuleResetReason | Supported values:<br>unknown(1)<br>powerUp(2)<br>parityError(3)<br>manualReset(5) |
| **cefcModuleTable (flash and fan tray entities)** | |
| • cefcModuleAdminStatus<br>• cefcModuleOperStatus<br>• cefcModuleResetReason | These objects not implemented. |
| **cefcMIBNotifications** | |
| • cefcPowerStatusChange | Not implemented. |

# CISCO-ENTITY-PFE-MIB

The CISCO-ENTITY-PFE-MIB contains objects to monitor the performance of the packet forwarding engine (PFE). PFE technology accelerates certain IP features in order to improve network performance. On the Cisco 10000 series ESR, the PFE is the parallel express forwarding network processor (PXF), which is part of the performance routing engine (PRE). This is the processor listed in the ENTITY-MIB entPhysicalTable.

There are no constraints on this MIB.

The CISCO-ENTITY-PFE-MIB maintains information about performance, performance trends, and PFE-related events. The MIB also summarizes the utilization and efficiency information provided by the **`show hardware pxf cpu context`** command. You can also use the MIB to set thresholds for utilization and efficiency, and monitor when those thresholds are exceeded. For instructions, see the "Monitoring PXF Utilization" section on page A-18.

The following CISCO-ENTITY-PFE-MIB tables contain information about processor performance:

- cePfePerfCurrentTable—Utilization and efficiency percentages: current, 1-minute, and 5-minute.
- cePfePerfIntervalTable—Performance statistics for the past 24 hours, in 15-minute intervals. The table holds 96 measurement intervals, less if the PXF has not been running for 24 hours.

  The start of each 15-minute interval is based on the time that the PXF was last started or restarted, which may not match the start of a quarter-hour increment in real time (for example, 10:45 or 11:15). For example, if the PXF was started at 10:20, subsequent 15-minute intervals start at 10:35, 10:50, and so on.
- cePfePerfTotalTable—Utilization and efficiency for the past 24 hours.

Several other MIB tables and objects are used to monitor PXF restarts and threshold-exceeded events:

- cePfePerfConfigTable—Settable thresholds for PXF utilization and efficiency limits. If a threshold is exceeded, SNMP generates an event and performs a user-configurable action.
- cePfePerfCurrentTable—Utilization and efficiency percentages: current, 1-minute, and 5-minute.
- cePfeHistTable—Information about threshold-exceeded events and PXF restarts.

- cePfeHistNotifiesEnable—The action that SNMP performs when a threshold is exceeded or the PXF is restarted.
- HistEventType—The list of events that can occur during PXF operation.

# CISCO-ENTITY-VENDORTYPE-OID-MIB

The CISCO-ENTITY-VENDORTYPE-OID-MIB defines the object identifiers (OIDs) assigned to Cisco 10000 series ESR components. The OIDs in this MIB are used in the ENTITY-MIB as values for the entPhysicalVendorType field in entPhysicalTable. Each OID uniquely identifies a type of physical entity (for example, a fan tray, power supply, or line card).

## MIB Constraints

Table 3-16 lists the objects and OIDs in the CISCO-ENTITY-VENDORTYPE-OID-MIB that describe router entities. For detailed definitions of MIB objects, see the MIB.

*Table 3-16 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Notes*

| MIB Object (OID Assignment) | Notes |
|---|---|
| **cevChassis** | |
| • cevChassis10008 (1.3.6.1.4.1.9.12.3.1.3.303) | Cisco 10008 chassis |
| **cevContainer** | |
| • cevContainerC10KSlot (1.3.6.1.4.1.9.12.3.1.5.86) | Line card and PRE slots |
| • cevContainerC10KPowerSupplySlot (1.3.6.1.4.1.9.12.3.1.5.87) | Power supply bays |
| • cevContainerC10KFanTraySlot (1.3.6.1.4.1.9.12.3.1.5.88) | Fan assembly slots |
| • cevContainerC10KFlashCardSlot (1.3.6.1.4.1.9.12.3.1.5.89) | Flash card slots |
| **cevPowerSupply** | |
| • cevPowerSupplyC10KDC (1.3.6.1.4.1.9.12.3.1.6.55) | DC power supply |
| • cevPowerSupplyC10KAC (1.3.6.1.4.1.9.12.3.1.6.56) | AC power supply |
| **cevFan** | |
| • cevFanTrayC10008 (1.3.6.1.4.1.9.12.3.1.7.25) | Cisco 10008 fan tray |
| **cevSensor** | |
| • cevSensorC10KInletTemp (1.3.6.1.4.1.9.12.3.1.8.22) | Inlet temperature sensor |
| • cevSensorC10KCoreTemp (1.3.6.1.4.1.9.12.3.1.8.23) | Core temperature sensor |

*Table 3-16 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Notes (continued)*

| MIB Object (OID Assignment) | Notes |
|---|---|
| **cevModule** | |
| cevModuleCpuType | |
| • cevCpuCreRp (1.3.6.1.4.1.9.12.3.1.9.5.29) | Central Routing Engine—Route Processor |
| • cevCpuCreFp (1.3.6.1.4.1.9.12.3.1. 9.5.30) | Central Routing Engine—Forwarding Processor |
| cevModule10000Type | |
| • cevPos1oc12 (1.3.6.1.4.1.9.12.3.1.9.32.1) | 1-port OC-12 Packet over SONET (POS) line card |
| • cevP6Ct3 (1.3.6.1.4.1.9.12.3.1.9.32.2) | 6-port channelized T3 line card |
| • cevGe (1.3.6.1.4.1.9.12.3.1.9.32.3) | 1-port gigabit Ethernet line card |
| • cevAtm1Oc12 (1.3.6.1.4.1.9.12.3.1.9.32.4) | 1-port OC-12 ATM line card |
| • cevP1COc12 (1.3.6.1.4.1.9.12.3.1.9.32.5) | 1-port channelized OC-12 line card |
| • cevP4Chstm1 (1.3.6.1.4.1.9.12.3.1.9.32.6) | 4-port channelized STM-1 line card |
| • cevPos6oc3 (1.3.6.1.4.1.9.12.3.1.9.32.13) | 6-port OC-3 POS line card |
| • cevAtm4oc3 (1.3.6.1.4.1.9.12.3.1.9.32.14) | 4-port OC-3 ATM line card with single-mode fiber, intermediate reach optics |
| • cevP8E3Ds3 (1.3.6.1.4.1.9.12.3.1.9.32.15) | 8-port unchannelized switchable T3/E3 line card |
| • cevSrpPos1oc48SmSr (1.3.6.1.4.1.9.12.3.1.9.32.16) | 1-port OC-48 SRP or POS SM short reach line card |
| • cevC10K48MbFlashCard (1.3.6.1.4.1.9.12.3.1.9.32.18) | 48 Mb flash card |
| • cevC10K128MbFlashCard (1.3.6.1.4.1.9.12.3.1.9.32.19) | 128 Mb flash card |
| • cevP24ChE1T1 (1.3.6.1.4.1.9.12.3.1.9.32.22) | 24-port channelized E1/T1 line card |
| • cevP8Fe (1.3.6.1.4.1.9.12.3.1.9.32.30) | 8-port fast Ethernet half-height line card |
| • cevP8Ds3E3Atm (1.3.6.1.4.1.9.12.3.1.9.32.31) | 8-port E3/DS3 ATM line card |
| • cevGe1h (1.3.6.1.4.1.9.12.3.1.9.32.33) | 1-port gigabit Ethernet half-height line card |
| **cevPort** | |

*Table 3-16 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Notes (continued)*

| MIB Object (OID Assignment) | Notes |
|---|---|
| • cevPortFEIP (1.3.6.1.4.1.9.12.3.1.10.16) | Fast Ethernet port |
| • cevPortT3 (1.3.6.1.4.1.9.12.3.1.10.20) | Channelized T3 and E3/DS3 line card port |
| • cevPortOC3SUNI (1.3.6.1.4.1.9.12.3.1.10.26) | OC-3 ATM line card port |
| • cevPortOC12SUNI (1.3.6.1.4.1.9.12.3.1.10.27) | OC-12 ATM line card port |
| • cevPortPOS (1.3.6.1.4.1.9.12.3.1.10.52) | OC-3 POS, OC-12 POS, OC-48 POS line card port |
| • cevPortGe (1.3.6.1.4.1.9.12.3.1.10.109) | Gigabit Ethernet line card port |
| • cevPortChOc12 (1.3.6.1.4.1.9.12.3.1.10.110) | Channelized OC-12 line card port |
| • cevPortChOc3Stm1 (1.3.6.1.4.1.9.12.3.1.10.111) | Channelized OC-3/STM-1 line card port |
| • cevPortChE1T1 (1.3.6.1.4.1.9.12.3.1.10.114) | Channelized E1/T1 line card port |
| • cevPortDs3E3Atm (1.3.6.1.4.1.9.12.3.1.10.125) | E3/DS3 ATM line card port |

# CISCO-ENVMON-MIB

The CISCO-ENVMON-MIB contains information about the status of environmental sensors (for voltage, temperature, fans, and power supplies). It also contains MIB objects to enable and disable notifications for changes to the status of these sensors.

When a router temperature test point reaches a critical state, the environmental monitor initiates a shutdown and sends a ciscoEnvMonShutdownNotification if it has been configured to do so (see the "Enabling Notifications" section on page 4-2).

## MIB Constraints

Table 3-17 lists the constraints that the router places on objects in the CISCO-ENVMON-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-17 CISCO-ENVMON-MIB Constraints*

| MIB Object | Notes |
|---|---|
| ciscoEnvMonPresent | Added c10000(10) as a supported chassis. |
| **ciscoEnvMonVoltageStatusTable** | Not implemented. |
| **ciscoEnvMonFanStatusTable** | |

*Table 3-17 CISCO-ENVMON-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • ciscoEnvMonFanStatusIndex | Always 1. Only one table row supported for fan tray. |
| • ciscoEnvMonFanStatusDescr | Always Fan Tray. |
| • ciscoEnvMonFanState | Supported values:<br>normal(1)—Both fans are working.<br>warning(2)—One fan is failing.<br>critical(3)—Both fans are failing.<br>notPresent(5)—Fan tray is missing.<br>notFunctioning(6)—Unable to get status. |
| **ciscoEnvMonSupplyStatusTable** | |
| • ciscoEnvMonSupplyStatusIndex | The value 1 indicates PEM0 and 2 indicates PEM1. |
| • ciscoEnvMonSupplyStatusDescr | Valid values are PEM0 or PEM1. |
| • ciscoEnvMonSupplyState | Supported values:<br>normal(1)—Power supply is working.<br>critical(3)—Power supply is failing.<br>notPresent(5)—Power supply is missing. |
| • ciscoEnvMonSupplySource | Supported values:<br>unknown(1)—Missing or unknown power supply.<br>ac(2)—AC power supply.<br>dc(3)—DC power supply. |
| ciscoEnvMonAlarmContacts | Not implemented. |
| ciscoEnvMonEnableVoltageNotification<br>ciscoEnvMonVoltageNotification | These objects not implemented. |

# CISCO-FLASH-MIB

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

There are no constraints on this MIB.

# 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.

The Cisco Frame Relay Management Information Base (MIB) describes managed objects that let you monitor Frame Relay operations remotely by using Simple Network Management Protocol (SNMP). The Frame Relay MIB Enhancements feature extends the Cisco Frame Relay MIB by adding MIB objects that monitor the following Frame Relay functionality:

- Frame Relay fragmentation
- Frame Relay-ATM Network Interworking (FRF.5)

- Frame Relay-ATM Service Interworking (FRF.8)
- Frame Relay switching
- Input and output rates of individual virtual circuits (VCs)

There are no constraints on this MIB.

# CISCO-FTP-CLIENT-MIB

The CISCO-FTP-CLIENT-MIB contains objects to invoke File Transfer Protocol (FTP) operations for network management.

There are no constraints on this MIB.

# CISCO-HSRP-EXT-MIB

The CISCO-HSRP-EXT-MIB provides an extension to the CISCO-HSRP-MIB. It contains objects to perform functions such as assigning secondary HSRP IP addresses, monitoring the operational status of interfaces, and modifying an HSRP group's priority.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# 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.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# CISCO-IETF-ATM2-PVCTRAP-MIB

The CISCO-IETF-ATM2-PVCTRAP-MIB supplements the ATM-MIB. It implements the virtual channel link (VCL) section of the IETF document "draft-ietf-atommib-atm2-11.txt," Section 9 ATM Related Trap Support.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN

The CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN contains information for monitoring ATM interfaces that is not defined in the ATM-MIB or the CISCO-IETF-ATM2-PVCTRAP-MIB.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# CISCO-IF-EXTENSION-MIB

CISCO-IF-EXTENSION-MIB contains objects which provide additional information about interfaces not available in other MIBS. This MIB extends the IF-MIB (RFC2863).

There are no constraints on this MIB.

# CISCO-IMAGE-MIB

The CISCO-IMAGE-MIB identifies the characteristics and capabilities of the Cisco IOS software image running on the router.

There are no constraints on this MIB.

# CISCO-IPMROUTE-MIB

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

There are no constraints on this MIB.

# 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 IP local 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 following command:

```
router(config)#snmp-server host <ip-address> <community-name> iplocalpool
```

The ciscoIpLocalPoolInUseAddrNoti notification is enabled:

- Through SNMP by using the cIpLocalPoolNotificationsEnable object
- Using the following CLI configuration:

  ```
  router(config)#snmp-server enable traps ip local pool
  ```

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

http://wwwin-eng.cisco.com/Eng/IOS/SNMP_WWW/mib-police/cgi-bin/showmib.cgi?action=show_mib&mib_name=CISCO-IP-LOCAL-POOL-MIB&version=3.1

# CISCO-IP-STAT-MIB

The CISCO-IP-STAT-MIB contains objects to manage the collection and display of IP statistics, categorized by IP precedence and the Media Access Control (MAC) address associated with IP packets. To use the MIB to access additional IP statistics, you can issue the **ip accounting mac-address** and **ip accounting precedence** commands at the CLI.

There are no constraints on this MIB.

# CISCO-IP-TAB-MIB

The CISCO-IP-TAB-MIB contains objects to manage the collection and display of IP statistics, categorized by IP precedence and the MediA.

# CISCO-IP-URPF-MIB

The CISCO-IP-URPF-MIB(Unicast Reverse Path Forwarding ) contains objects that allows users to specify a 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 3-18 lists constraints in the CISCO-IP-URPF-MIB.

*Table 3-18 CISCO-IP-URPF-MIB Object Groups*

| MIB Tables | Description |
|---|---|
| **cipUrpfIfMonTable** | Entries in these 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 these 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-MEMORY-POOL-MIB

The CISCO-MEMORY-POOL-MIB contains objects to monitor memory pools on the router.

There are no constraints on this MIB.

# CISCO-NETFLOW-MIB

The CISCO-NETFLOW-MIB contains objects that remotely obtains and manages cache flow information, current NetFlow configuration, and statistics.

The Netlow MIB provides a simple and easy method to get NetFlow cache information, current NetFlow configuration and statistics.The MIB provides Netflow information in these areas:

- Cache information and configuration

- Export information and configuration
- Export Statistics
- Protocol Statistics
- Top Flows information

Table 3-19 lists object groups supported in the CISCO-NETFLOW-MIB in order to to manage informative and configurable parameters.

*Table 3-19 CISCO-NETFLOW-MIB Object Groups*

| Objects Group | Description |
|---|---|
| cnfCacheInfo | Provides common information for all active/inactive flows ( i.e. entries, time out etc) per cache basis. |
| cnfExportInfo | Provides information about export like export version and export destinations(/Collectors). |
| cnfFeatureAcceleration | Provides information about NetFlow Feature Acceleration. |
| cnfExportStatistics | Provides export statistics. |
| cnfProtocolStatistics | Provides a summary of NetFlow cache statistics. |
| cnfExportTemplate | Provides Template based Version 9 flow export information and statistic. |

SNMP is used to collect network information. SNMP permits retrieval of critical information from network elements such as routers, switches, and workstations. The CISCO-NETFLOW-MIB feature uses SNMP to configure NetFlow and to gather NetFlow statistics.

The CISCO-NETFLOW-MIB contains objects that allow NetFlow statistics and other NetFlow data for the managed devices on your system to be retrieved by SNMP. You can specify retrieval of NetFlow information from a managed device (for example, a router) either by entering commands on that managed device or by entering SNMP commands from the NMS workstation to configure the router through the MIB.

If the NetFlow information is configured from the NMS workstation, no access to the router is required and all configuration can be performed through SNMP. The CISCO-NETFLOW-MIB request for information is sent from an NMS workstation through SNMP to the router and is retrieved from the router. This information is stored or viewed, thus allowing NetFlow information to be easily accessed and transported across a multivendor programming environment.

The CISCO-NETFLOW-MIB feature defines managed objects that enable a network administrator to remotely monitor the following NetFlow information:

- Flow cache configuration information
- NetFlow export information
- General NetFlow statistics

**Note** For detailed information about the CISCO-NETFLOW-MIB, go to: http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00805e11ab.html

# CISCO-OAM-MIB

The CISCO-OAM-MIB contains objects to configure cell-based Operations, Administration, and Maintenance (OAM) loopback ping tests on ATM connections. The MIB also contains information about test results.

The Cisco 10000 series ESR can run 100 ping tests at one time. If you attempt to run more than 100 ping tests, the router queues excess tests and runs them as other tests finish.

## MIB Constraints

Table 3-20 lists the constraints that the router places on objects in the CISCO-OAM-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-20 CISCO-OAM-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **oamLoopbackPingTable** | |
| • oamLoopbackPingLocation | Maximum octet string size is 12 bytes, not 16 bytes. |

# 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. There are no constraints on this MIB.

# CISCO-PING-MIB

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

There are no constraints on this MIB.

# 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 3-21 lists the constraints that the router places on objects in the CISCO-PPPOE-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-21 CISCO-PPPOE-MIB Constraints*

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

# CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB displays memory and CPU usage on the router, and describes active system processes.

## MIB Constraints

The router places the following constraint on the CISCO-PROCESS-MIB:

- CPU statistics in the cpmCPUTotalTable are maintained only for the active Performance Routing Engine (PRE). Statistics are not maintained for the standby PRE or for line cards.

  This means that cpmCPUTotalPhysicalIndex is always the index of the active PRE.

# CISCO-PRODUCTS-MIB

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

There are no constraints on this MIB.

Table 3-22 lists the MIB objects added to the CISCO-PRODUCTS-MIB to support the Cisco 10000 series ESR. The MIB includes an OID definition for c10400. However, the OID definition is meaningless because c10400 is not a valid product ID. For detailed definitions of MIB objects, see the MIB.

*Table 3-22 CISCO-PRODUCTS-MIB New OID Assignments*

| MIB Object (OID Assignment) | Notes |
|---|---|
| cisco10008 (1.3.6.1.4.1.9.1.438) | New object for Cisco 10008 Internet Router. |

# CISCO-QINQ-VLAN-MIB

The CISCO-QINQ-VLAN-MIB defines configuration and monitoring capabilities relating to 802.1 QinQ interfaces. QinQ interfaces terminate QinQ traffic and translate QinQ tags. The IEEE 802.1Q VLAN specification provides for an option to tag Ethernet frames with two VLAN tags:

- CE VLAN—An inner tag that specifies the customer's VLAN ID.
- PE VLAN (metro tag)—An outer tag that specifies the service provider's VLAN ID.

The combination of inner and outer VLAN tags is used to uniquely identify a particular customer's service flow.

## MIB Constraints

Table 3-23 lists the constraints that the Cisco 10000 series ESR places on objects in the CISCO-QINQ-VLAN-MIB. Unless noted otherwise, the Cisco 10000 series implementation of a MIB follows the standard. Any objects not listed in a table are implemented as defined in the MIB.

*Table 3-23 CISCO-QINQ-VLAN-MIB Constraints*

| MIB Object | Notes |
|---|---|
| cqvTerminationRowStatus | Read only. |
| cqvTerminationPeEncap | Read only |

# CISCO-QUEUE-MIB

The CISCO-QUEUE-MIB contains objects to manage interface queues on the router.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# 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 3-24 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 3-24 lists the constraints that the router places on objects in the CISCO-RTTMON-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-24 CISCO-RTTMON-MIB Constraints*

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

# CISCO-SNAPSHOT-MIB

The CISCO-SNAPSHOT-MIB contains objects to manage snapshot routing, which helps improve the use of system resources for static routing and routing for dedicated serial lines.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# 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 10000 series ESR to send syslog messages to a 'syslog' server.

## MIB Constraints

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

# CISCO-SSG-MIB

The CISCO-SSG-MIB contains objects to manage the Service Selection Gateway (SSG) product on the router. SSG enables service providers to offer subscribers access to the Internet, corporate networks, and value-added services through broadband access technology such as digital subscriber lines (DSL), cable modems, and wireless access.

SSG works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM), to:

- Authenticate the access rights of subscribers
- Provide subscribers with a selection of services available to them
- Connect subscribers to services

Subscribers can:

- Dynamically connect to and disconnect from services (which can be public or private)
- Concurrently connect to a number of different services

SSG communicates with the authentication, authorization, and accounting (AAA) management network where RADIUS, Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside. SSG also communicates with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

## MIB Constraints

Table 3-25 lists the constraints that the router places on objects in the CISCO-SSG-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-25 CISCO-SSG-MIB Constraints*

| MIB Object | Notes |
|---|---|
| ssgCfgLocalForwarding | Not supported. |
| ssgCfgAutoDomainNat | Not supported. |
| ssgCfgTransPassThrough | Not supported. |
| ssgCfgMaxServicesPerUser | The router supports a maximum of 7 services per service group. Each user can only be subscribed to one service group. |
| ssgCfgTcpRedirGrpForSMTP | Not supported. |
| ssgCfgTcpRedirGrpForAdvCapt | Not supported. |
| **ssgServiceTable** | |
| • ssgServiceDNSPrimaryIpType<br>• ssgServiceDNSPrimary<br>• ssgServiceDNSSecondaryIpType<br>• ssgServiceDNSSecondary | DNS redirect is not supported for these table objects. |

# CISCO-TAP2-MIB

The CISCO-TAP2-MIB contains objects to manage the Transmission Control Protocol (TCP) on the router. This MIB is an extension to the IEisco IOS software image.

# CISCO-TCP-MIB

The CISCO-TCP-MIB contains objects to manage the Transmission Control Protocol (TCP) on the router. This MIB is an extension to the IETF TCP MIB.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# CISCO-VPDN-MGMT-EXT-MIB

The CISCO-VPDN-MGMT-EXT-MIB supplements the CISCO-VPDN-MGMT-MIB with additional information about VPDN tunnels and sessions. The MIB contains the following tables, which provide read-only information not found in the CISCO-VPDN-MGMT-MIB:

- cvpdnTunnelExtTable—Provides information about Layer 2 Tunnel Protocol (L2TP) tunnels, such as tunnel statistics and User Datagram Protocol (UDP) port numbers.
- cvpdnSessionExtTable—Provides information about L2TP sessions, as well as information about session packet counts, packet sequencing information, window size, and operating characteristics.

## MIB Constraints

Table 3-26 lists the constraints that the router places on objects in the CISCO-VPDN-MGMT-EXT-MIB. In addition, the MIB is read-only, which means that you cannot use the MIB to configure VPDN on the router.

*Table 3-26 CISCO-VPDN-MGMT-EXT-MIB Constraints*

| MIB Object | Notes |
|---|---|
| All MIB objects | Read-only. |
| **cvpdnSessionExtTable** | |
| • cvpdnSessionRemoteSendSequence<br>• cvpdnSessionRemoteRecvSequence<br>• cvpdnSessionSentZLB<br>• cvpdnSessionRecvZLB<br>• cvpdnSessionSentRBits<br>• cvpdnSessionRecvRBits<br>• cvpdnSessionLocalWindowSize<br>• cvpdnSessionRemoteWindowSize<br>• cvpdnSessionCurrentWindowSize<br>• cvpdnSessionMinimumWindowSize<br>• cvpdnSessionATOTimeouts<br>• cvpdnSessionOutGoingQueueSize<br>• cvpdnSessionAdaptiveTimeOut<br>• cvpdnSessionRoundTripTime<br>• cvpdnSessionPktProcessingDelay<br>• cvpdnSessionZLBTime | These objects not implemented. |

# 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 3-27 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 3-27 have been deprecated. Although currently supported, their use is being phased out and we recommend that you use the replacement object instead. For detailed definitions of MIB objects, see the MIB.

*Table 3-27 CISCO-VPDN-MGMT-MIB Constraints*

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

# DS1-MIB

The DS1-MIB provides access to configuration and performance monitoring information for DS1 controllers and interfaces on the router.

## MIB Constraints

Table 3-28 lists the constraints that the router places on objects in the DS1-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-28 DS1-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **dsx1ConfigTable** | |
| • dsx1LineType | Read-only. For Channelized OC-12 and channelized T3 line cards, supported values are:<br>• dsx1ESF(2)<br>• dsx1D4(3) |
| • dsx1LineCoding | Read-only. Supports dsx1B8ZS(2) value only. |

*Table 3-28 DS1-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • dsx1SendCode | Read-only. Supports dsx3SendNoCode value only. |
| • dsx1CircuitIdentifier | Read-only. Always NULL. |
| • dsx1LoopbackConfig | Read-only. |
| • dsx1SignalMode | Read-only. Always defaults to the value none(1). |
| • dsx1TransmitClockSource | Read-only. |
| • dsx1Fdl | Read-only. |
| • dsx1LineLength | Read-only. |
| • dsx1LineStatusChangeTrapEnable | Read-only. |
| • dsx1Channelization | Read-only. |
| **dsx1FracTable** | Not implemented. Deprecated. |

# DS3-MIB

The DS3-MIB provides access to configuration and performance monitoring information for DS1 controllers and interfaces. The Cisco 10000 series ESR supports the version of the MIB based on RFC 2496.

## MIB Constraints

Table 3-29 lists the constraints that the router places on objects in the DS3-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-29 DS3-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **dsx3ConfigTable** | |
| • dsx3LineType | Supported values are:<br>• dsx3other(1)<br>• dsx3M23(2)<br>• dsx3CbitParity(4) |
| • dsx3LineCoding | Read-only. Supports dsx3B3ZS(2) value only. |
| • dsx3SendCode | Read-only. Supports dsx3SendNoCode value only. |
| • dsx3CircuitIdentifier | Read-only. Always NULL. |
| • dsx3LoopbackConfig | Read-only. |
| • dsx3InvalidInterval | Always 0 for any line card. |
| • dsx3Ds1ForRemoteLoop | Always 0, which has no effect because dsx3SendCode does not support dsx3SendDs1LoopCode. |
| **dsx3FarEndConfigTable** | Not implemented. |

*Table 3-29 DS3-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| **dsx3FarEndCurrentTable** | Not implemented. |
| **dsx3FarEndIntervalTable** | Not implemented. |
| **dsx3FarEndTotalTable** | Not implemented. |
| **dsx3FracTable** | Not implemented. Deprecated. |

# ENTITY-MIB

The ENTITY-MIB contains objects that represent only physical entities (components) in the router and allows SNMP management of those entities. The current software release supports the RFC 2037 version of this MIB.

The MIB table entPhysicalTable identifies the physical entities in the router. The entPhysicalTable contains a single row for the Cisco 10000 chassis and a row for each entity in the chassis. A physical entity may contain other entities (for example, a fan-tray bay may contain a fan-tray module, which may contain one or more fans). The physical hierarchy of system components is determined at runtime, based on the actual router configuration.

## MIB Constraints

Table 3-30 lists the constraints that the router places on objects in the ENTITY-MIB. For detailed definitions of MIB objects, see the MIB. Any MIB table or object not listed in a constraint table is implemented as defined in the MIB.

*Table 3-30 ENTITY-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **entPhysicalTable** | |
| • entPhysicalAlias<br>• entPhysicalAssetID | Not implemented. |
| **entLogicalTable** | Not implemented. |
| **entLPMappingTable** | Not implemented. |

## ENTITY-MIB UDI Support

The ENTITY-MIB 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 unique device identifier is comprised of an orderable product identifier (PID), the version identifier (VID), and the hardware Serial Number (SN). The UDI is stored in IDPROM. The PID, VID, and SN must be stored in the entPhysicalTable:

- PID shall be stored in the entPhysicalModelName object
- VID shall be stored in the entPhysicalHardwareRev object

- SN shall be stored in the entPhysicalSerialNum object

**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. See for a complete description of the Cisco UDI feature.

Each product that is capable of MIB support is required to populate ENTITY-MIB v2 or later with PID, VID, and SN. This compliance is also a requirement of the Consistent Network Element Manageability initiative. If the product uses both ENTITY-MIB and CISCO-ENTITY-ASSET-MIB, then the data in the following fields should be identical.

ENTITY-MIB v2 (RFC-2737) fields to be populated are:

- Entity-MIB.entPhysicalName (Product Name)
- Entity-MIB.entPhysicalDescr (Product Description)
- Entity-MIB.entPhysicalModelName (PID)
- Entity-MIB.entPhysicalHardwareRev (VID)
- Entity-MIB.entPhysicalSerialNumber (SN)

### ENTITY-MIB Usage

The following MIB entities are dependent on each user's configuration:

- entPhysicalIndex—Uniquely identifies each entity in the router. The index is also used to access information about the entity in other MIB tables.
- entPhysicalContainedIn—Indicates the entPhysicalIndex of a component's parent entity. The value of entPhysicalIndex for the physical entity which 'contains' this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity.
- entPhysicalParentRelPos—An integer that shows the relative position of same-type entities that have the same entPhysicalContainedIn value (for example, slots and line card ports).
- entPhysicalDescr—A textual description of a physical entity. This object should contain a string which identifies the manufacturer's name for the physical entity and should be set to a specific value for each version or model of the physical entity..

# ETHERLIKE-MIB

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

## MIB Constraints

Table 3-31 lists the constraints that the router places on objects in the ETHERLIKE-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-31 ETHERLIKE-MIB Constraints*

| MIB Object | Notes |
|---|---|
| dot3StatsTable | |

*Table 3-31 ETHERLIKE-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • dot3StatsSQETestErrors | Always 0. |
| • dot3StatsInternalMacTransmitErrors | Always 0. |
| • dot3StatsEtherChipSet | Deprecated object. Always NULL. |
| **dot3CollTable** | Not implemented. |

# EVENT-MIB

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

There are no constraints on this MIB.

# EXPRESSION-MIB

The EXPRESSION-MIB contains objects to define expressions of MIB objects for network management purposes.

There are no constraints on this MIB.

# IF-MIB

The IF-MIB contains objects to manage physical and logical interfaces. The Cisco 10000 series ESR supports the ifGeneralInformationGroup of MIB objects for all layers.

The IF-MIB provides index, statistics, and stacking information for physical interfaces, subinterfaces, and Layer 2 protocols on the Cisco 10000 series ESR. The ifStackTable shows the relationship between protocol layers and their underlying physical or virtual interfaces, with each layer and sublayer represented in the ifTable.

For example, an MPLS-layer interface is stacked above the physical or virtual interface passing MPLS traffic, and MPLS traffic-engineered tunnels are stacked above the MPLS-layer interface.

## MIB Constraints

The router fully supports the MIB as it is defined in RFC 2233, with the specifications described in Table 3-32.

*Table 3-32 IF-MIB Constraints*

| MIB Object | Notes |
|---|---|
| ifDescr | The T1 layer is defined as:<br>T1 slot/subslot/port |
| | The T3 layer is defined as:<br>T3 slot/subslot/port |
| | The SONET layer is defined as one of the following:<br>POS slot/subslot/port<br>CH-SONET slot/subslot/port<br>CH-OC12 slot/subslot/port<br>SONET slot/subslot/port |
| ifType | The following definitions were added:<br>• ds1(18)—T1 layer<br>• ds3(30)—T3 layer<br>• sonet(39)—SONET layer |
| ifSpeed | The following definitions were added:<br>T1 layer:<br>ds1(1544000)<br>e1(2048000)<br>T3 layer:<br>ds3(44736000)<br>e3(34368000)<br>SONET layer:<br>SONET/SDH line rate (for example, 155520000 bps) |
| ifPhysAddress | Set to the value of the circuit identifier. If no circuit identifier exists, an octet string with zero length. |
| ifAdminStatus | The following administrative states are supported:<br>up(1)<br>down(2) |

*Table 3-32 IF-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| ifOperStatus | The value testing(3) not supported for any layer.<br>T1 layer:<br>ifOperStatus set to down(2) if interface line status is not dsx1NoAlarm(1).<br>T3 layer:<br>ifOperStatus set to down(2) if interface line status is not dsx3NoAlarm(1).<br>SONET layer:<br>ifOperStatus set to down(2) if sonetSectionCurrentStatus and sonetLineCurrentStatus are not sonetSectionNoDefect(1) and sonetLineNoDefect(1), respectively. |
| ifLastChange | The value of sysUpTime when ifOperStatus last changed. |
| ifName | Nonvolatile alias name assigned to interface by administrator. |
| ifLinkUpDownTrapEnable | Set to enabled(1). |
| ifHighSpeed | Speed of line in megabits per second: 2, 6, or 8. |
| ifConnectorPresent | Set to true(1) for physical interface, false(2) for others. |

# IGMP-MIB

The IGMP-MIB contains objects to manage the Internet Group Management Protocol (IGMP) on the router.

There are no constraints on this MIB.

# INT-SERV-GUARANTEED-MIB

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

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# INT-SERV-MIB

The INT-SERV-MIB describes the Integrated Services Protocol (ISP).

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# IP-MIB

The IP-MIB contains objects to manage physical and logical interfaces. The Cisco 10000 series ESR supports the ifGeneralInformationGroup of MIB objects for all layers.

The IP-MIB provides index, statistics, and stacking information for physical interfaces, subinterfaces, and Layer 2 protocols on the Cisco 10000 series ESR. The ifStackTable shows the relationship between protocol layers and their underlying physical or virtual interfaces, with each layer and sublayer represented in the ifTable..

# IP-FORWARD-MIB

The IP-FORWARD-MIB contains objects to display classless interdomain routing (CIDR) multipath IP routes.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# IPMROUTE-MIB

The IPMROUTE-MIB contains objects to manage IP multicast routing on the router, independent of the actual multicast routing protocol in use.

There are no constraints on this MIB.

# MPLS-LDP-MIB

The MPLS-LDP-MIB provides management information for the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP), which is used by label switching routers (LSRs) to communicate the definitions of labels that each router is using. The router supports the IETF draft version of this MIB (draft-ietf-mpls-ldp-mib-08.txt).

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st21/ldpmib21.htm

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# MPLS-LSR-MIB

The MPLS-LSR-MIB provides configuration and performance monitoring information to manage label switched paths (LSPs) through a label switching router (LSR) remotely. The MPLS-LSR-MIB enables you to display the contents of the the Label Forwarding Information Base (LFIB).

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st14/lsrmib.htm

# MIB Constraints

Table 3-33 lists the constraints that the router places on objects in the MPLS-LSR-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-33 MPLS-LSR-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **mplsInterfaceConfTable** | |
| • mplsInterfaceConfStorageType | Read-only. |
| **mplsInterfacePerfTable** | |
| • mplsInterfaceInPackets<br>• mplsInterfaceInDiscards<br>• mplsInterfaceInFailedLabelLookup<br>• mplsInterfaceOutLabelsUsed<br>• mplsInterfaceOutPackets<br>• mplsInterfaceOutDiscards<br>• mplsInterfaceOutFragments | These objects not implemented. Not available in hardware. |
| **mplsInSegmentTable** | |
| • mplsInSegmentAdminStatus | Read-only. |
| **mplsInSegmentPerfTable** | |
| • mplsInSegmentOctets<br>• mplsInSegmentPackets<br>• mplsInSegmentHCOctets | These objects not implemented. Not available in hardware. |
| **mplsOutSegmentTable** | |
| • mplsOutSegmentIfIndex<br>• mplsOutSegmentPushTopLabel<br>• mplsOutSegmentTopLabel<br>• mplsOutSegmentNextHopIpAddrType<br>• mplsOutSegmentNextHopIpv4Addr<br>• mplsOutSegmentNextHopIpv6Addr<br>• mplsOutSegmentOwner<br>• mplsOutSegmentTrafficParamPtr<br>• mplsOutSegmentRowStatus<br>• mplsOutSegmentStorageType<br>• mplsOutSegmentAdminStatus | These objects read-only. |
| **mplsOutSegmentPerfTable** | |
| • mplsOutSegmentOctets<br>• mplsOutSegmentPackets<br>• mplsOutSegmentHCOctets | These objects not implemented. Not available in hardware. |

*Table 3-33 MPLS-LSR-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **mplsXCTable** | |
| • mplsXCLspId | These objects read-only. |
| • mplsXCLabelStackIndex | |
| • mplsXCIsPersistent | |
| • mplsXCOwner | |
| • mplsXCRowStatus | |
| • mplsXCStorageType | |
| • mplsXCAdminStatus | |
| **mplsLabelStackTable** | |
| • mplsLabelStackLabel | These objects read-only. |
| • mplsLabelStackRowStatus | |
| • mplsLabelStackStorageType | |
| **mplsTrafficParamTable** | |
| • mplsTrafficParamMaxRate | These objects not implemented. |
| • mplsTrafficParamMeanRate | |
| • mplsTrafficParamMaxBurstSize | |
| • mplsTrafficParamRowStatus | |
| • mplsTrafficParamStorageType | |
| **Trap enables** | |
| • mplsInSegmentTrapEnable | These objects not implemented. |
| • mplsOutSegmentTrapEnable | |
| • mplsXCTrapEnable | |
| **Traps** | |
| • mplsInSegmentUp | These objects not implemented. |
| • mplsInSegmentDown | |
| • mplsOutSegmentUp | |
| • mplsOutSegmentDown | |
| • mplsXCUp | |
| • mplsXCDown | |

# MPLS-TE-MIB

The MPLS-TE-MIB enables the Cisco 10000 series ESR to perform traffic engineering for MPLS tunnels. The Cisco 10000 series ESR supports the IETF draft version of this MIB (draft-ietf-mpls-te-mib-05.txt).

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

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008008705e.html

# MIB Constraints

Table 3-34 lists the constraints that the router places on objects in the MPLS-TE-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-34 MPLS-TE-MIB Constraints*

| MIB Object | Notes |
|---|---|
| mplsTunnelMaxHops | Always 65535. |
| **mplsTunnelTable** | |
| • mplsTunnelName | Read-only. |
| • mplsTunnelDescr | Read-only. |
| • mplsTunnelIsIf | Read-only. |
| • mplsTunnelXCPointer | Read-only. |
| • mplsTunnelSignallingProto | Always rsvp(2). |
| • mplsTunnelSetupPrio | Read-only. |
| • mplsTunnelHoldingPrio | Read-only. |
| • mplsTunnelSessionAttributes | Read-only. |
| • mplsTunnelOwner | Read-only. |
| • mplsTunnelLocalProtectInUse | Always false(2). |
| • mplsTunnelResourcePointer | Read-only. |
| • mplsTunnelInstancePriority | Always 0. |
| • mplsTunnelHopTableIndex | Read-only. |
| • mplsTunnelIncludeAnyAffinity | Always 0. |
| • mplsTunnelIncludeAllAffinity | Read-only. |
| • mplsTunnelExcludeAllAffinity | Read-only. |
| • mplsTunnelPathInUse | Read-only. |
| • mplsTunnelRole | Read-only. |
| • mplsTunnelTotalUpTime | Read-only. |
| • mplsTunnelInstanceUpTime | Always 0. |
| • mplsTunnelAdminStatus | Always up(1). |
| • mplsTunnelOperStatus | Always up(1). |
| • mplsTunnelRowStatus | Read-only. |
| • mplsTunnelStorageType | Always readOnly(5). |
| mplsTunnelHopListIndexNext | Always 0. |
| **mplsTunnelHopTable** | |
| • mplsTunnelHopAddrType | Always ipV4(1). |

*Table 3-34 MPLS-TE-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| • mplsTunnelHopIpv4Addr | Read-only. |
| • mplsTunnelHopIpv4PrefixLen | Read-only. |
| • mplsTunnelHopIpv6Addr | Read-only. |
| • mplsTunnelHopIpv6PrefixLen | Read-only. |
| • mplsTunnelHopAsNumber | Read-only. |
| • mplsTunnelHopLspId | Read-only. |
| • mplsTunnelHopType | Always strict(1). |
| • mplsTunnelHopRowStatus | Read-only. |
| • mplsTunnelHopStorageType | Always readOnly(5). |
| mplsTunnelResourceIndexNext | Not supported. Always 0. |
| **mplsTunnelResourceTable** | |
| • mplsTunnelResourceMaxRate | Read-only. |
| • mplsTunnelResourceMeanRate | Read-only. |
| • mplsTunnelResourceMaxBurstSize | Always 1000. |
| • mplsTunnelResourceRowStatus | Read-only. |
| • mplsTunnelResourceStorageType | Always readOnly(5). |
| **mplsTunnelARHopTable** | |
| • mplsTunnelARHopAddrType | Always ipV4(1). |
| • mplsTunnelARHopType | Always strict(1). |
| **mplsTunnelCHopTable** | |
| • mplsTunnelCHopAddrType | Always ipV4(1). |
| • mplsTunnelCHopType | Always strict(1). |
| mplsTunnelIndexNext | Always 0. |

# MPLS-VPN-MIB

The MPLS VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers.

The MPLS-VPN-MIB contains objects that are used to:

- Model an MPLS BGP Virtual Private Network (VPN)
- Provision VPN routing/forwarding instances (VRFs) on MPLS interfaces
- Monitor routes and route targets for each VRF
- Measure the performance of MPLS/BGP VPNs

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

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1829/products_feature_guide09186a008016108a.html#wp1027129

# MIB Constraints

Table 3-35 lists the constraints that the router places on objects in the MPLS-VPN-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-35 MPLS-VPN-MIB Constraints*

| MIB Object | Notes |
|---|---|
| mplsVpnVrfConfMaxPossibleRoutes | Always 0 (not supported). |
| **mplsVpnInterfaceConfTable** | Read-only. |
| • mplsVpnInterfaceLabelEdgeType | Always providerEdge(1). |
| • mplsVpnInterfaceConfStorageType | Always volatile(2). |
| • mplsVpnInterfaceConfRowStatus | Always active(1). |
| **mplsVpnVrfTable** | Read-only. |
| • mplsVpnVrfConfRowStatus | Always active(1). |
| • mplsVpnVrfConfStorageType | Always volatile(2). |
| **mplsVpnVrfRouteTargetTable** | Read-only. |
| • mplsVpnVrfRouteTargetRowStatus | Always active(1). |
| **mplsVpnVrfBgpNbrAddrTable** | Read-only. |
| • mplsVpnVrfBgpNbrType | Always ipv4(1). |
| • mplsVpnVrfBgpNbrRowStatus | Always active(1). |
| • mplsVpnVrfBgpNbrStorageType | Always volatile(2). |
| **mplsVpnVrfBgpNbrPrefixTable** | Not implemented. |
| **mplsNumVrfSecTable** | Not supported. Hardware does not have an illegal label RX counter. |
| **mplsVpnVrfRouteTable** | Read-only. |
| • mplsVpnVrfRouteDestAddrType | Always ipv4(1). |
| • mplsVpnVrfRouteMaskAddrType | Always ipv4(1). |
| • mplsVpnVrfRouteTos | Always 0. |
| • mplsVpnVrfRouteNextHopAddrType | Always ipv4(1). |
| • mplsVpnVrfRouteInfo | Always 0.0 (not supported). |
| • mplsVpnVrfRouteNextHopAS | Always 0 (not supported). |
| • mplsVpnVrfRouteMetric2 | Supported only for Cisco IGRP and EIGRP; otherwise, value is –1. |
| • mplsVpnVrfRouteMetric3 | Supported only for Cisco IGRP and EIGRP; otherwise, value is –1. |
| • mplsVpnVrfRouteMetric4 | Supported only for Cisco IGRP and EIGRP; otherwise, value is –1. |
| • mplsVpnVrfRouteMetric5 | Supported only for Cisco IGRP and EIGRP; otherwise, value is –1. |
| • mplsVpnVrfRouteRowStatus | Always active(1). |
| • mplsVpnVrfRouteStorageType | Always volatile(2). |

*Table 3-35 MPLS-VPN-MIB Constraints (continued)*

| MIB Object | Notes |
|---|---|
| **Notifications** | |
| mplsNumVrfSecIllegalLabelThreshExceeded | Not supported. Hardware does not have an illegal label RX counter. |

# 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/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt5msdp.htm

## MIB Constraints

Table 3-36 lists the constraints that the router places on objects in the MSDP-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-36 MSDP-MIB Constraints*

| MIB Object | Notes |
|---|---|
| **msdpRequestsTable** | Not supported. |
| **msdpTraps** | |
| • msdpEstablished | Not supported. |
| All other MIB objects | Read-only. |

# NOTIFICATION-LOG-MIB

The NOTIFICATION-LOG-MIB contains information about SNMP notifications (traps and informs).

## MIB Constraints

The objects in this MIB are read-only. You must configure SNMP notification log functionality through CLI commands such as **snmp mib notification-log default**, **snmp mib notification-log default disable**, **snmp mib notification-log globalageout**, and **snmp mib notification-log globalsize**.

You can view the contents of a notification log through SNMP by reading the nlmLogTable; or, you can use the CLI command **show snmp mib-notification log**.

Table 3-37 lists the constraints that the router places on objects in the NOTIFICATION-LOG-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-37 NOTIFICATION-LOG-MIB Constraints*

| MIB Object | Notes |
|---|---|
| nlmConfigGlobalEntryLimit | Read-only. |
| nlmConfigGlobalAgeOut | Read-only. |
| **nlmConfigLogTable** | The current implementation supports a default log only; named logs are not supported. |

# OLD-CISCO-CHASSIS-MIB

The OLD-CISCO-CHASSIS-MIB describes chassis objects in devices running an older implementation of the Cisco IOS operating system. Those objects are now described in the ENTITY-MIB. This MIB is deprecated.

# OLD-CISCO-CPU-MIB

The OLD-CISCO-CPU-MIB describes CPU usage and active system processes on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-INTERFACES-MIB

The OLD-CISCO-INTERFACES-MIB contains objects to manage interfaces on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-IP-MIB

The OLD-CISCO-IP-MIB contains objects to manage IP on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-MEMORY-MIB

The OLD-CISCO-MEMORY-MIB contains objects that describe memory pools on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-SYSTEM-MIB

The OLD-CISCO-SYSTEM-MIB provides information about system resources on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-TCP-MIB

The OLD-CISCO-TCP-MIB contains information about the TCP implementation on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OLD-CISCO-TS-MIB

The OLD-CISCO-TS-MIB contains objects to manage terminals and terminal lines on devices running an older implementation of the Cisco IOS operating system. This MIB is deprecated.

# OSPF-MIB

The OSPFM-MIB contains objects to manage Protocol Independent Multicast (PIM) on the router. The OSPF-MIB supports the latest RFC 1850 and adds the latest draft extensions.

# PIM-MIB

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

There are no constraints on this MIB.

# QINQ-VLAN-MIB

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

There are no constraints on this MIB.

# 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. Theis platform supports the IP part of RFC1213 and a draft of RFC2011 (draft-ietf-ipngwg-rfc2011-update-00), the CISCO-IETF-IP-MIB.

There are no constraints on this MIB.

# RFC1253-MIB

The RFC1253-MIB contains objects to manage version 2 of the Open Shortest Path First (OSPF) protocol.

There are no constraints on this MIB.

# RFC1315-MIB

The 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 3-38 lists the constraints that the router places on objects in the RFC1315-MIB. For detailed definitions of MIB objects, see the MIB.

*Table 3-38 RFC1315-MIB Constraints*

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

# RMON-MIB

The RMON-MIB contains objects to remotely monitor devices in the network.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# RS-232-MIB

The RS232-MIB contains objects to manage RS-232-like hardware interfaces and devices.

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# RSVP-MIB

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

Although this MIB is included in the Cisco IOS software image, the MIB is currently not supported for broadband configurations.

# SNMP-FRAMEWORK-MIB

The SNMP-FRAMEWORK-MIB contains objects that describe the SNMP management architecture.

There are no constraints on this MIB.

# SNMP-MPD-MIB

The SNMP-MPD-MIB contains statistics for SNMP message processing and dispatching processes on the router.

There are no constraints on this MIB.

# SNMP-NOTIFICATION-MIB

The SNMP-NOTIFICATION-MIB contains managed objects for SNMP v3 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.

There are no constraints on this MIB.

# SNMP-PROXY-MIB

The SNMP-PROXY-MIB 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.

There are no constraints on this MIB.

# SNMP-TARGET-MIB

The SNMP-TARGET-MIB 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).

There are no constraints on this MIB.

# SNMP-USM-MIB

The SNMP-USM-MIB contains objects that describe the SNMP User-based Security Model.

There are no constraints on this MIB.

# SNMPv2-MIB

The SNMPv2-MIB contains objects to manage SNMP v2 entities on the router.

There are no constraints on this MIB.

# SNMP-VACM-MIB

The SNMP-VACM-MIB contains objects that describe the view-based access control model for SNMP.

**Note** To access this MIB, you must create an SNMP v3 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
```

There are no constraints on this MIB.

# SONET-MIB

The SONET-MIB contains objects to manage SONET/SDH interfaces on the router.

There are no constraints on this MIB.

# TCP-MIB

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

There are no constraints on this MIB.

# UDP-MIB

The UDP-MIB contains objects to manage the User Datagram Protocol (UDP) on the router.

There are no constraints on this MIB.

CHAPTER 4

# Monitoring Notifications

This chapter describes the Cisco 10000 Series Routernotifications supported by the MIB enhancements feature introduced in Cisco IOS Release 12.2xxxx. 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

An SNMP agent can notify the manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, the agent:

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

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt 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 trap recipients. These recipients indicate where Network Registrar notifications are directed. By default, all notifications are enabled, but no trap recipients are defined. Until you define the recipients, no notifications are sent.

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

**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 this command.

Specify the trap types if you don't 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. The Event Table must have an entry that specifies the action that is to be performed.

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

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_1/
- http://www.cisco.com/warp/public/477/SNMP/SNMPTrapsInImages.html
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf014.htm

# Enabling Notifications

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

Command line interface (CLI)—Specify the recipient of the trap message and specify the types of traps sent. This command also specifies which types of informs are enabled.

- For detailed procedures, go to:
  - http://www.cisco.com/warp/public/477/SNMP/SNMPTrapsInImages.html
  - http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113t/113t_1/snmpinfm.htm
- Performing an SNMP SET operation using the **setany** command— To enable or disable MIB notifications, perform an SNMP **SET** operation on the 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:

- Text string—The event display
- Brief 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 required* is documented, there might be instances where an application, such as trouble ticketing occurs. For detailed information, go to the following URL: http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/info_ctr/3_0/install/overview.htm

# Environmental or Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco 10000 series ESR or conditions that might affect the router's functionality.

***Table 4-1 Environmental and 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 module command to view error message details. For Syslog messages associated with this event, consult Messages and Recovery Procedures. |
| | | A line card is provisioned for a slot but it is not present in the slot. | Insert a configured line card in the specific slot. |
| | | Module is operational | No action is required. |
| | | Module has failed due to some condition | Enter the show module 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 line cards, fan, port, power supply, or redundant power supply was added. | No action is required. |
| **cefcFRURemoved** | Indicates that a FRU was removed. | A field replaceable unit such as line cards, fan, ports, power supply, or redundant power supply was removed. | Replace the field replaceable unit. |

*Table 4-1 Environmental and Functional Notifications (continued)*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **chassisAlarmOn** | Indicates that a FRU status has changed. The chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has changed to the on (2) state. | The chassis temperature is too high, a minor or major alarm has been detected. | Inspect the indicated component closely to determine why it is operating out of the normal operating temperature range and whether it will eventually exceed the allowed operating temperature range. |
| | | A redundant power supply has been powered off. | Replace the field replaceable unit. |
| | Router's cooling fan could be close to failure. | One or more fans in the system fan tray have failed. Although this is a minor alarm, system components could overheat and be shut down. | Replace the fan as soon as possible or the system might shut itself down or fail to operate properly. |
| **chassisAlarmOff** | Indicates that a FRU status has changed. The chassisTempAlarm, chassisMinorAlarm, or chassisMajorAlarm object in this MIB has changed to the off (1) state. | A redundant power supply has been powered on. | No action required. |
| **ccCopyCompletion** | Indicates that a configuration copy operation completed. | The router finished copying a configuration file to or from another location. | |
| **ciscoConfigManEvent** | Indicates that a router configuration changed. | | |
| **dsx1LineStatusChange**<br>dsx3LineStatusChange | 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. |

# Cisco Line Card Notifications

These notifications indicate the failure of a line card or error conditions on the card that might affect the functionality of all interfaces and connected customers.

Table 4-2 lists ENTITY-MIB notifications generated by Cisco 10000 series ESR line cards.

*Table 4-2 Cisco 10000 Series Router Card Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **entConfigChange** | An entry for the line card is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change). | A line card was removed. | Replace the field replaceable unit. |
| | An entry for the line card is added to the entPhysicalTable (which causes the value of entLastchangeTime to change). | A line card was inserted. | No action required. |
| **cefcModuleOperStatus** | Indicates that the line card operational state changed. A management application uses this trap to update the status of a module that it is managing. | A line card is provisioned for a slot but it is not present in the slot. | Add a module. |
| **entSensorThresholdNotification** | Indicates that the sensor value crossed the threshold. This variable reports the most recent measurement seen by the sensor and This variable indicates the value of the threshold. | 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.<br>**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 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. |

*Table 4-2 Cisco 10000 Series Router Card Notifications (continued)*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **ceAssertAlarm** | The agent generates this trap when a physical entity asserts an alarm. | This alarm is sent for the following reasons:<br>• Fan failure, fan tray missing.<br>• Power entry module failure.<br>• Core or inlet temperature crosses a threshold, such as core critical temperature limit was reached.<br>• Sent when the alarm "Card Stopped Responding OIR" occurs.<br>• Path alarm indication signal occurs.<br>• Path remote failure indication occurs.<br>• Path loss of a pointer.<br>• Line alarm indication signal.<br>• Line remote failure indication.<br>• Section loss of signal failure.<br>• Threshold cross alarm.<br>• Out of frame failure.<br>• Signal failure<br>• Far end clock is out of range. | Check the entPhysicalDescr type and take the corresponding action; because there are many types of asserted alarms. |
| **ceClearAlarm** | 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.<br>• Sent when a line card is installed or removed in a line card slot and the alarm "Active Card Removed OIR" is cleared. | No action required. |

# Flash Card Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco 10000 series ESR flash cards. These notifications indicate the failure of a flash card or error conditions on the card that might affect the functionality of all interfaces and connected custom

*Table 4-3 Flash Card 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 card was inserted, check the ciscoFlashDeviceTable. |
| | Indicates a removable flash device is removed from the router. | Status change occurred. | To determine which flash card was inserted, check the ciscoFlashDeviceTable. |
| ciscoFlashCopyCompletionTrap | Indicates that a flash copy operation finished. | | |
| ciscoFlashPartitioningCompletionTrap | Indicates that a flash partitioning operation finished. | | |
| ciscoFlashMiscOpCompletionTrap | Indicates that a miscellaneous flash card operation finished such as ?????? | | |

# 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 can not transmit or receive traffic. The ifOperStatus object shows the link's 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).<br>Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**. |
| **linkUp** | Indicates that a link's status 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 link-down state during a switchover. | No action is required. |

# MPLS Service Notifications

Table 4-5 lists service notifications generated by the router to indicate conditions for services.

*Table 4-5 MPLS-Service Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **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.<br>May be caused by an administrative or operational status check of the tunnel. | No action is required. |
| **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) respectively. | A configured tunnel is transitioning to the down state.<br>May be caused by an administrative or operational status check of the tunnel. | |

*Table 4-5 MPLS-Service Notifications (continued)*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **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. |
| **VpnThreshCleared** | **This notifies the network administrator that the number of routes has changed.** | The number of routes in a VRF have fallen below the thresholds. | |

# Routing Protocol Notifications

Table 4-6 lists BGP4-MIB notifications which are Border Gateway Protocol (BGP) state changes generated by the Cisco 10000 series ESR to indicate error conditions for routing protocols and services.

*Table 4-6 Routing Protocol Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **bgpEstablished** | The BGP FSM enters the ESTABLISHED state. It becomes active on the router. | The BGP routing protocol changed status. | No action is required. |
| **bgpBackwardTransition** | Indicates that the BGP protocol 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. | The BGP routing protocol changed status. | This threshold value is configured using the CLI command, **neighbor <nbr_addr> <max_prefixes> [ theshold] [warning-only]** |

# Chassis Notifications

Table 4-7 lists CISCO-STACK-MIB notifications generated by the router to indicate that a chassis module has become active or stopped responding. These notifications are supported by the Cisco 10000 series router.

*Table 4-7 Chassis Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **moduleDown** | The status of a module changes from the OK state to another state. | The agent entity has detected that the moduleStatus object in this MIB has transitioned to the ok (2) state for one of its modules. The generation of this trap can be controlled by the sysEnableModuleTraps object in this MIB. | Enter the **show module command** and check the status. |
| **moduleUp** | The status of a module changes to the OK state. | The agent entity has detected that the moduleStatus object in this MIB has transitioned out of the ok (2) state for one of its modules. The generation of this trap can be controlled by the sysEnableModuleTraps object in this MIB. | No action required. |

# RTT Monitor Notifications

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

*Table 4-8 RTT Monitor Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **rttMonConnectionChangeNotification** | Sent when the value of rttMonCtrlOperConnectionLostOccurred changes. | Occurs when the connection to a target has either failed to be established or was lost and then re-established. | Check for the connectivity to the target. There could be link problems to the target through different hops. |
| **rttMonTimeoutNotification** | A timeout occurred or was cleared. | An RTT probe occurred and the system sends the notice when the value of rttMonCtrlOperTimeoutOccurred changes. | Check for the end-to-end connectivity if rttMonCtrlOperTimeoutOccurred if the notification returns true.<br>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 required. |

# Environmental Notifications

Table 4-9 lists CISCO-ENVMON-MIB notifications generated for events that might indicate the failure of the Cisco 10000 series ESR or conditions that might affect the router's functionality.

*Table 4-9 Environmental Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **ciscoEnvMonShutdownNotification** | A ciscoEnvMonShutdown Notification is sent if the environmental monitor detects a testpoint reaching a critical state and is about to initiate a shutdown. This notification contains no objects so that it may be encoded and sent in the shortest amount of time possible. Management applications should not rely on receiving such a notification as it may not be sent before the shutdown completes. | A test point nears a critical state and the router is about to shut down (for example, if auto-shutdown is enabled and the chassis core or inlet temperature reaches critical state and remains there for more than 2 minutes).<br>The system has a configuration to shut down a module if its operating temperature exceeds a temperature threshold. This configuration has been bypassed, and a module will still operate in an over-temperature condition. Operating at an over-temperature condition can damage the hardware. | Do not override the sensor alarms that act on an over-temperature condition. Enter the **environment-monitor shutdown temperature command** to bring the system back to standard temperature detection. |
| **ciscoEnvMonFanNotification** | | One or more fans in the system fan tray have failed. Although this is a minor alarm, system components could overheat and be shut down. | Replace the system fan tray. |
| **ciscoEnvMonRedundantSupplyNotification** | Sent if the redundant power supply (if available) fails. | An environmental condition, an over-temperature condition, or inconsistent voltage to the module occurred. Since such a notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification. | Ensure that the system power supplies are optimally redundant. Use power supplies with identical output ratings or reduce system power consumption. |

*Table 4-9 Environmental Notifications (continued)*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| ciscoEnvMonTempStatusChange Notif | The core or inlet temperature is outside its normal range, when ciscoEnvMonState is at the Warning or Critical state.<br>Since such a Notification is usually generated before the shutdown state is reached, it can convey more data and has a better chance of being sent than does the ciscoEnvMonShutdownNotification. | During previous reloads, this module experienced a timeout while accessing the temperature sensor. All further access to the temperature sensor will be disabled. This condition indicates a possible problem with the temperature sensor. | 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. |

* The cefcFRUPowerAdminStatus is on(1) when a redundant power supply is disabled. When there is a redundant power supply, the cefcFRUPowerAdminStatus is always on(1) for both power supplies, regardless if the redundant power supply is disabled.

# Frame Relay Notification

Table 4-10 lists notifications that can occur during router frame relay events.

*Table 4-10 Frame Relay Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| frDLCISStatusChange | Indicates that a virtual circuit has changed. | Sent when a Frame Relay virtual circuit changes status. For example, when a circuit is created or destroyed or its status changes between active and inactive. | |

# PFE Notifications

Table 4-11 lists notifications that can occur during PFE (packet forwarding engine) events.

*Table 4-11 PFE Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| **cePfeThldEvent** | Indicates that the PFE utilization or efficiency status changed. | Sent when PFE utilization or efficiency reaches or exceeds a threshold. For example, if the current PFE utilization (cePfePerfCurrentUtilization) reaches or exceeds the threshold cePfePerfConfigThldUtilization, SNMP generates a thldUtilizationEvent.<br><br>cePfeHistType indicates the type of event that occurred. See the MIB object HistEventType for details about event types. | Enable this notification through the CLI or by setting cePfeHistNotifiesEnable to notify(3) or logAndNotify(4). |
| **cePfeHistRestartEvent** | Indicates that the PFE processor status changed. | The PFE processor was restarted. | No action required. |

# Service Selection Gateway Notification

Table 4-12 lists notifications that can occur during service selection gateway (SSG) events.

*Table 4-12 Service Selection Gateway Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| | Indicates that SSG status has changed. | Sent when SSG detects that a RADIUS client has rebooted. (SSG uses RADIUS servers to authenticate subscribers.) | |

# Protocol Notifications

Table 4-13 lists notifications that can occur during protocol events.

*Table 4-13 Protocol Notifications*

| Event | Description | Probable Cause | Recommended Action |
|---|---|---|---|
| frDLCISStatusChange | Indicates that the casState object status has changed. | Sent when the casState object changes state. The value of casState indicates if the router should send requests to the authentication, authorization, and accounting (AAA) server:<br>• up(1)—Send requests to the server.<br>• dead(2)—Do not send requests to the server. Send requests to the next available server instead.<br>The object casState does not necessarily indicate the current state of the server. This is because casState is always up(1) unless an AAA request fails. In that case, casState is set to dead(2) and then reset to up(1) to allow the router to send requests to the server after a failure.<br>The number of minutes casState remains dead(2) is specified by the command **radius-server deadtime** *minutes*. For example, if server deadtime is 5 minutes and an AAA request fails, a notification is generated with casState set to dead(2). Five minutes later, another notification is generated with casState set to up(1) even though the server may still be down. | |
| oamLoopbackPingCompletionTrap | | Sent when an OAM loopback test is completed. | |
| cPppoeSystemSessionThresholdTrap | | Sent when the number of active PPPoE sessions exceeds the value of cPppoeSystemThresholdSessions | |
| **cPppoeVcSessionThresholdTrap** | | Sent when the number of active PPPoE sessions on the VC exceeds the value of cPppoeVcThresholdSessions | |

APPENDIX A

# Using MIBs

This chapter describes how to use SNMP to perform tasks on the Cisco 10000 series ESR. For information about how to avoid performance problems when you use SNMP to poll the router for routing table entries, see the "Considerations for Working with MIBs" section on page 2-1.



## Managing Physical Entities

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

- Generating SNMP Traps, page A-9

See the "Preprovisioning Line Cards" section on page A-20 for information about how to use SNMP to preconfigure the operating characteristics of a line card before the line card is inserted into the chassis.

### Purpose and Benefits

The physical entity management feature of the Cisco 10000 SNMP implementation does the following:

- Organizes the physical entities in the chassis into a containment tree that describes the relationship of each entity to all other entities
- 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-ASSET-MIB—Contains asset tracking information (ID PROM contents) for the physical entities listed in the entPhysicalTable of the ENTITY-MIB. The MIB provides device-specific information for physical entities, including orderable part number, serial number, manufacturing assembly number, and hardware, software, and firmware information.
- 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.

**Note** Currently, the CISCO-ENTITY-FRU-CONTROL-MIB supports only line cards.

- CISCO-ENTITY-VENDORTYPE-OID-MIB—Contains the object identifiers (OIDs) for all physical entities in the router.
- CISCO-ENVMON-MIB—Contains information about the status of environmental sensors (for voltage, temperature, fans, and power supplies). For example, this MIB reports the chassis core and inlet temperatures.
- 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.

# Performing Inventory Management

Perform a MIB walk on the ENTITY-MIB entPhysicalTable to obtain information about entities in the router.

Figure A-1 through Figure A-5 show how entries in the entPhysicalTable provide information about entities.

## Notes about entPhysicalTable Entries

As you examine 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). (See Figure A-5.)

## Sample entPhysicalTable Entries

The figures in this section show how information is stored in the entPhysicalTable. You can determine the router configuration by examining entPhysicalTable entries.

Figure A-1 shows the ENTITY-MIB entPhysicalTable entries for a Gigabit Ethernet line card installed in slot 1 of the router chassis, and for the port on that line card.

***Figure A-1 entPhysicalTable Entries for Chassis Entities***

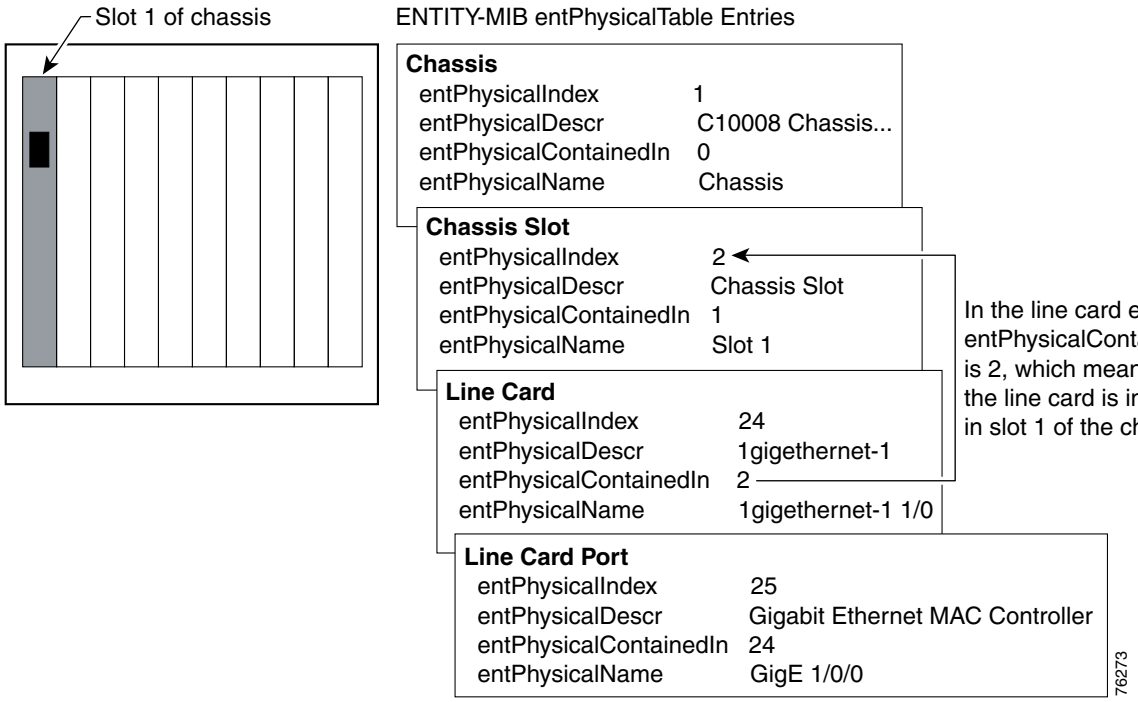



Figure A-2 shows sample entPhysicalTable entries for the entities shown in Figure A-4 and Figure A-5.

*Figure A-2 Sample entPhysicalTable Entries*

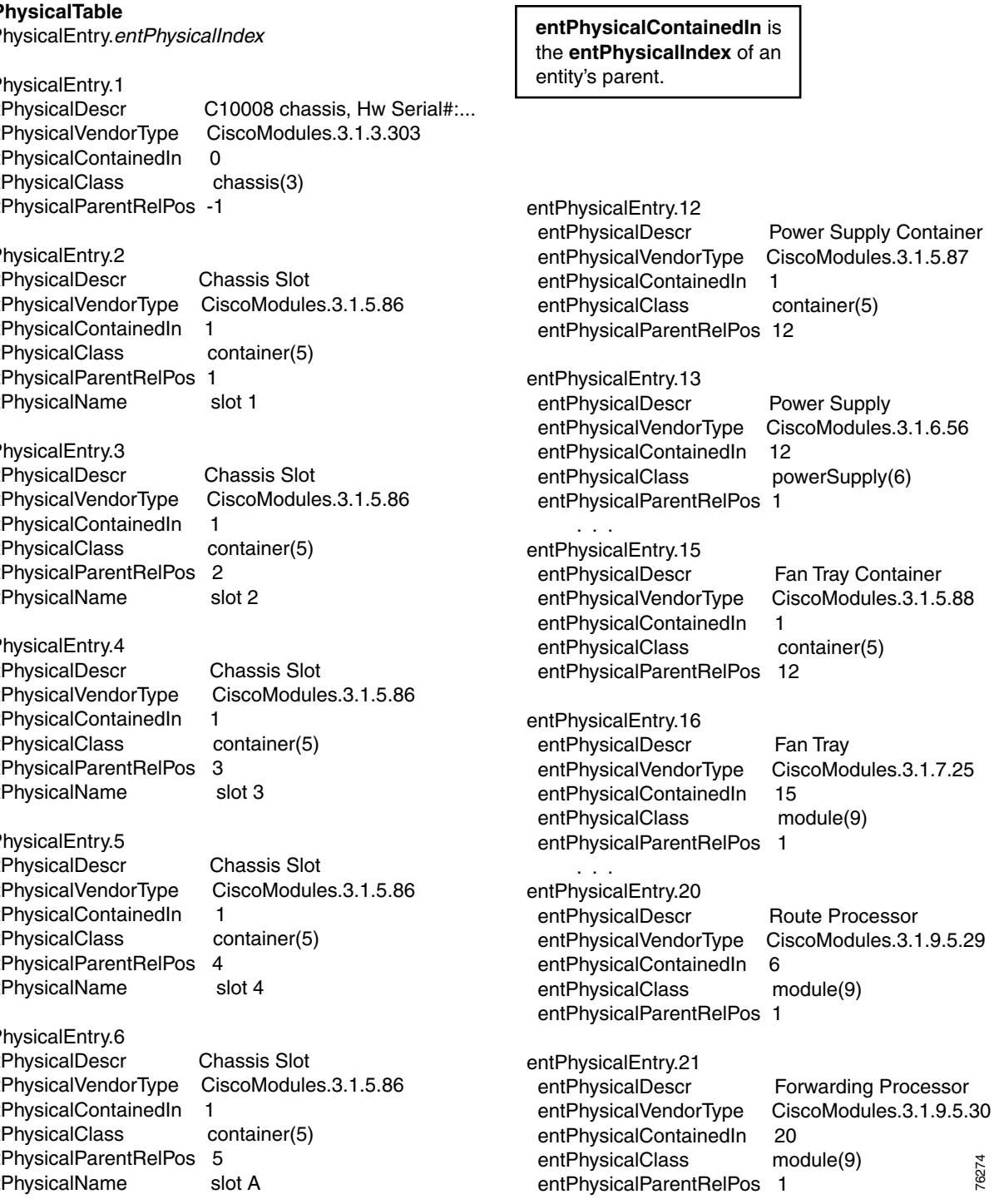


*Figure A-3 Sample entPhysicalTable Entries (continued)*

**entPhysicalTable** *(continued)*
entPhysicalEntry.*entPhysicalIndex*

entPhysicalEntry.24
entPhysicalDescr 1gigethernet-1
entPhysicalVendorType CiscoModules.3.1.9.32.3
entPhysicalContainedIn 2
entPhysicalClass module(9)
entPhysicalParentRelPos 1

entPhysicalEntry.25
entPhysicalDescr Gigabit Ethernet MAC Controller
entPhysicalVendorType CiscoModules.3.1.10.109
entPhysicalContainedIn 24
entPhysicalClass port(10)
entPhysicalParentRelPos 1
entPhysicalName GigE 1/0/0

entPhysicalEntry.26
entPhysicalDescr 6cht3-1
entPhysicalVendorType CiscoModules.3.1.9.32.2
entPhysicalContainedIn 3
entPhysicalClass module(9)
entPhysicalParentRelPos 1

entPhysicalEntry.27
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 1
entPhysicalName Serial2/0/0

entPhysicalEntry.28
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 2
entPhysicalName Serial2/0/1

entPhysicalEntry.29
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 3
entPhysicalName Serial2/0/2

entPhysicalEntry.30
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 4
entPhysicalName Serial2/0/3

entPhysicalEntry.31
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 5
entPhysicalName Serial2/0/4

entPhysicalEntry.32
entPhysicalDescr PMC FREEM, PMC S/UNI...
entPhysicalVendorType CiscoModules.3.1.10.20
entPhysicalContainedIn 26
entPhysicalClass port(10)
entPhysicalParentRelPos 6
entPhysicalName Serial2/0/5

entPhysicalEntry.33
entPhysicalDescr 1oc12pos-1
entPhysicalVendorType CiscoModules.3.1.9.32.1
entPhysicalContainedIn 4
entPhysicalClass module(9)
entPhysicalParentRelPos 1

entPhysicalEntry.34
entPhysicalDescr Skystone 4302 Sonet Framer
entPhysicalVendorType CiscoModules.3.1.10.52
entPhysicalContainedIn 33
entPhysicalClass port(10)
entPhysicalParentRelPos 1
entPhysicalName POS3/0/0

76275

Figure A-4 shows the entPhysicalTable entries for all of the line cards and line card ports in the configuration.

*Figure A-4 entPhysicalTable Entries for Line Cards and Line Card Ports*

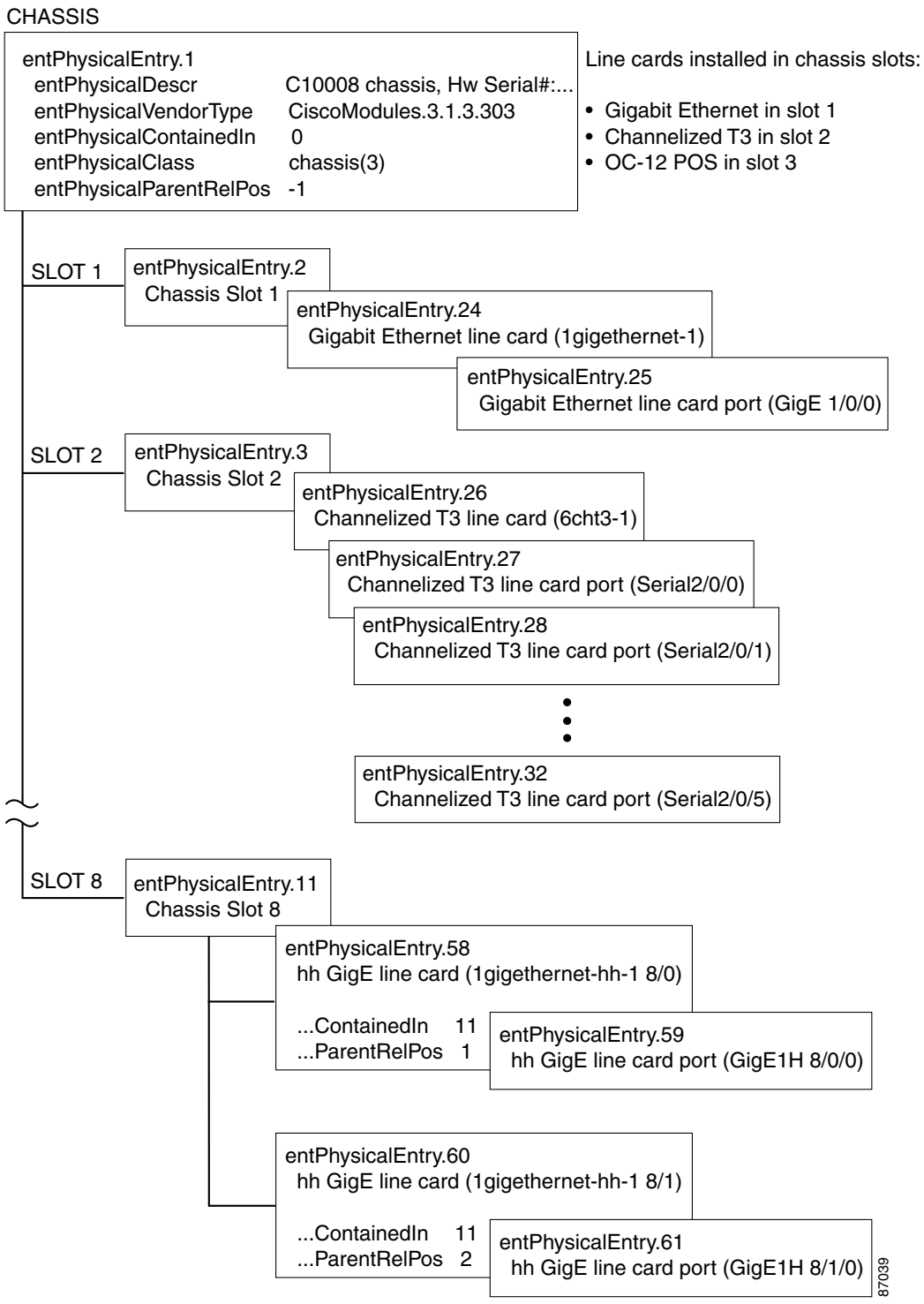
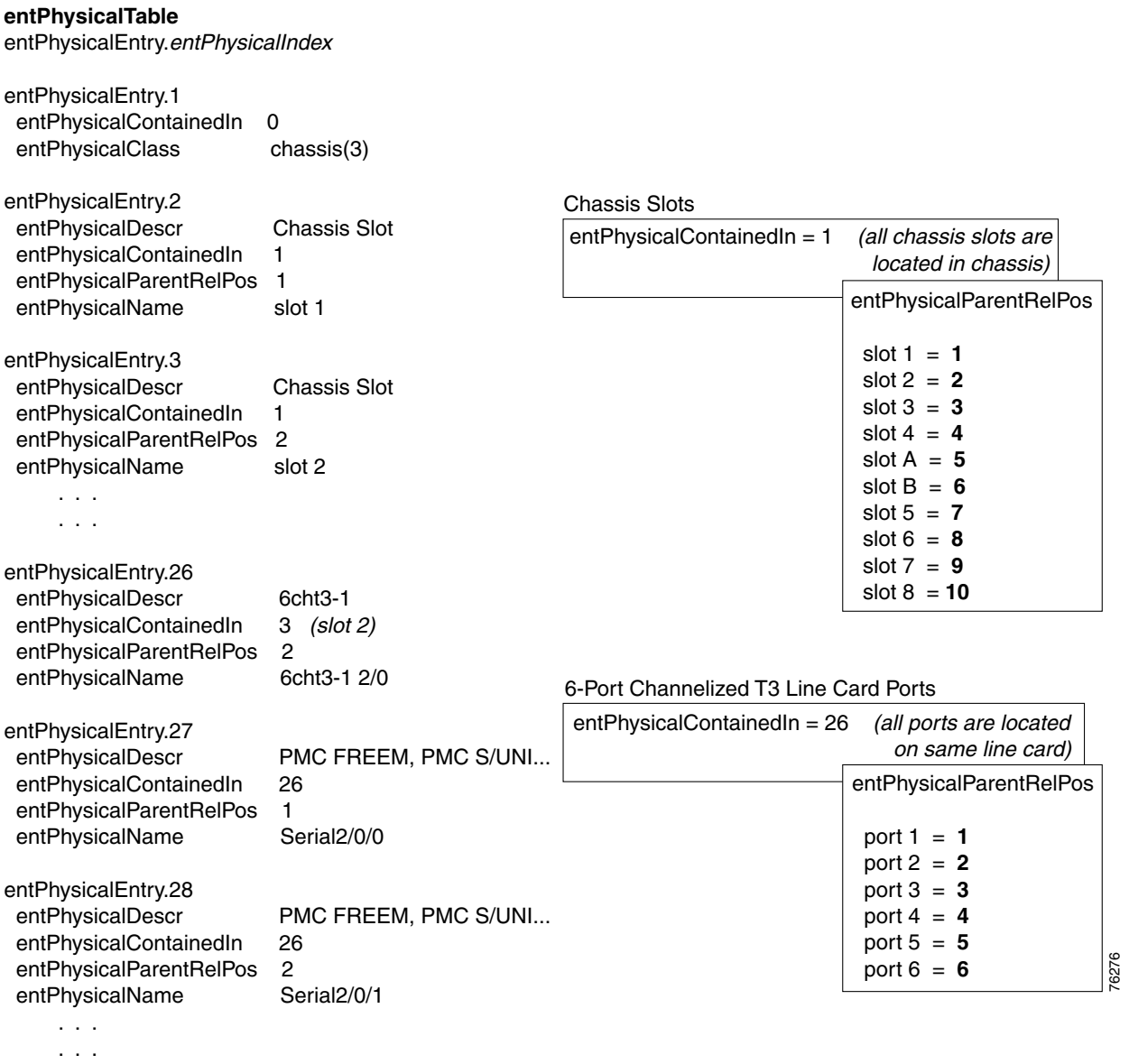



Figure A-5 shows how entPhysicalParentRelPos indicates the position of same-type entities within their parent object. Note that the entPhysicalTable entries on the left include relevant fields only.

*Figure A-5 entPhysicalParentRelPos Values for Chassis Slots*




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 line card ports, entPhysicalContainedIn = 26 (the entPhysicalIndex of the line card).
- Each chassis slot and line card port has a different entPhysicalParentRelPos to show its relative position within the parent object.
- The 6-port channelized T3 line card is installed in slot 2 of the chassis.

## 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. For example, 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.35.0 = ifIndex.4
```

## Tagging Router Assets

You can use the CISCO-ENTITY-ASSET-MIB **ceAssetTag** object to assign a unique, nonvolatile identifier (tag) to any line card or Performance Routing Engine (PRE) that you want to keep track of. The tag remains with the PRE or line card even if it is installed in another chassis.

For example, the following ceAssetTable entry shows an asset tag of `pre-1-1ge` being assigned to the Gigabit Ethernet line card whose serial number is `CAB0430AXEU`. Even if the line card is removed from this chassis and installed in another chassis, its ceAssetTag remains `pre-1-1ge`.

```
ceSerialNumber = CAB0430AXEU
ceOrderablePartNumber = ESR-1GE
ceAssetTag = pre-1-1ge
  .  .  .
```

# 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.

**Note** Currently, the CISCO-ENTITY-FRU-CONTROL-MIB supports only line cards. For additional MIB constraints, see the "CISCO-ENTITY-FRU-CONTROL-MIB" section on page 3-18.

Figure A-6 shows a cefcModuleTable entry for a Gigabit Ethernet line card whose entPhysicalIndex is 24.

***Figure A-6 Sample cefcModuleTable Entry***

```
cefcModuleEntry.entPhysicalIndex

cefcModuleEntry.24
  cefcModuleAdminStatus = enabled(1)
  cefcModuleOperStatus = ok(2)
  cefcModuleResetReason = manual reset(5)
  cefcModuleStatusLastChangeTime = 7714
```

See the "FRU Status Changes" section on page A-10 for information about how the router generates traps to indicate changes in FRU status.

# Generating SNMP Traps

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



## Identifying Hosts to Receive Traps

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 (traps 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: trap(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 traps. For example, to generate mplsLdpSessionUp or mplsLdpSessionDown traps, the MPLS-LDP-MIB object mplsLdpSessionUpDownTrapEnable must be set to enabled(1).

## Configuration Changes

If entity traps are enabled, the router generates an entConfigChange trap (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 should occasionally check the value of entLastChangeTime (ENTITY-MIB) to detect any entConfigChange traps that were missed due to throttling or transmission loss.

#### Enabling Traps for Configuration Changes

To configure the router to generate an entConfigChange trap whenever its configuration changes, enter the following command from the CLI. Use the **no** form of the command to disable the traps.

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

## Environmental Conditions

The CISCO-ENVMON-MIB sends the following traps to alert you to conditions detected by environmental sensors in the router:

- ciscoEnvMonShutdownNotification—Sent when the router is about to shut down.
- ciscoEnvMonTemperatureNotification—Sent when a temperature is outside its normal range.
- ciscoEnvMonFanNotification—Sent when a fan fails.
- ciscoEnvMonRedundantSupplyNotification—Sent when a redundant Power Entry Module fails.

#### Enabling Environmental Traps

To configure the router to generate traps for environmental conditions, enter the following command from the CLI. Use the **no** form of the command to disable the traps.

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

To enable environmental traps through SNMP, set the appropriate notification enable object to true(1). For example, ciscoEnvMonEnableShutdownNotification enables shutdown notifications. Disable the traps by setting the notification object to false(2).

## FRU Status Changes

If FRU traps are enabled, the router generates the following traps in response to changes in the status of an FRU. See the CISCO-ENTITY-FRU-CONTROL-MIB for more information about these traps.

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

#### Enabling FRU Traps

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

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

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

# Using Alarms to Monitor Outages

The Cisco 10000 series ESR generates alarms to indicate a condition such as the loss of a signal on a SONET path or the activation of a T1 interface on a channelized T3 line card. Alarms also provide status information for router entities, and alert users to conditions that might degrade network performance or cause a failure (an *outage*).

Alarm messages are sent to the console, and information about alarms is also maintained in the CISCO-ENTITY-ALARM-MIB, which is described later in this section. Each physical entity in the entPhysicalTable (ENTITY-MIB) has a set of alarms that define conditions that can occur on the entity.

This section provides basic information about alarms, and it includes the following subsections:

- Viewing Active Alarms Through the CLI
- Using the CISCO-ENTITY-ALARM-MIB to Monitor Alarms

For information about how to monitor router interfaces for problems, see the "Monitoring Router Interfaces" section on page A-16.

**Note** An alarm indicates a condition, not an event. For example, the alarm "Core critical temperature limit" indicates that the chassis core temperature has reached critical state.

### Purpose and Benefits

Using the alarm monitoring feature, you can:

- Monitor when alarms are asserted and cleared
- Obtain alarm history information
- Track alarm statistics and counts
- Generate SNMP traps and syslog messages in response to alarms

### MIBs and Alarm Subsystems Used to Monitor Alarms

The router monitors alarms using:

- CISCO-ENTITY-ALARM-MIB—Alarms for physical entities defined in the ENTITY-MIB entPhysicalTable.
- CISCO-SYSLOG-MIB—Contains objects to monitor syslog messages through SNMP.
- Cisco IOS alarm subsystem—Alarms for physical entities.
- Omega alarm subsystem—Alarms for logical entities and interfaces (for example, T1 interfaces on a channelized T3 line card).

## Alarm Overview

Each alarm contains the following information:

- Alarm type—A unique code that identifies the alarm.
- Severity—The seriousness of the condition causing the alarm (see the following "Viewing Active Alarms Through the CLI" section for more information).

- Description—Information about the condition that caused the alarm.

### Alarm States

An alarm's state indicates the current state of the condition that caused the alarm:

- Asserted—The condition currently exists.
- Cleared—The condition has been resolved.

SNMP uses the following traps to indicate the current state of an alarm:

- ceAlarmAsserted—The condition that caused the alarm still exists.
- ceAlarmCleared—The condition that caused the alarm has been resolved.

By default, an SNMP trap and syslog message are generated each time an alarm is asserted or cleared. You can, however, set the severity level of alarms for which traps and syslog messages are generated, or disable the traps and messages completely (see the "Enabling Traps and Syslog Messages for Alarms" section on page A-16).

### Alarm Severity Descriptions

The severity of an alarm indicates the type of condition that the alarm represents:

- critical(1)—A severe, service-affecting condition requiring immediate corrective action.
- major(2)—A hardware or software condition that causes a serious disruption of service, or is on hardware essential to the operation of the router. Although less serious than a critical alarm, a major alarm requires immediate attention to correct the problem.
- minor(3)—A condition or problem that does not affect service, or is on nonessential hardware.
- info(4)—An informational message about an event that improves operation, or an indication of a condition that could cause a problem.

## Viewing Active Alarms Through the CLI

To view information about all active alarms on the router, enter the following command from the CLI (where *severity* is the level of alarms to display). The router displays all active alarms with this severity level and higher. If you do not specify *severity*, all active alarms are displayed.

```
Router(config)# show facility-alarm status [ severity ]
```

## Using the CISCO-ENTITY-ALARM-MIB to Monitor Alarms

The CISCO-ENTITY-ALARM-MIB allows you to monitor alarms on the router through SNMP.

**Note** The CISCO-ENTITY-ALARM-MIB monitors alarms only for physical entities defined in the entPhysicalTable (ENTITY-MIB). Alarms for logical entities, such as channelized interfaces, are monitored by Cisco IOS software through syslog.

The MIB contains several tables and objects that provide information about alarms:

- ceAlarmDescrMapTable—Assigns a unique index (ceAlarmDescrIndex) to each physical entity to identify the entity's alarms (see Figure A-7). The table contains an entry for each entity identified by entPhysicalVendorType in the entPhysicalTable (ENTITY-MIB).

- ceAlarmDescrTable—Contains a description of each alarm that every physical entity can generate.
- ceAlarmTable—Lists the alarms currently being asserted by each physical entity on the router, and contains alarm control information for the entity.
- ceAlarmHistTable—Contains a history of the alarms that have occurred on the router.
- ceAlarmCriticalCount—The number of critical alarms currently asserted on the router. The router also maintains numeric counts of major (ceAlarmMajorCount) and minor (ceAlarmMinorCount) alarms.

The MIB also contains objects to control how the router responds to alarms:

- ceAlarmCutOff—Enables you to turn off audible alarms controlled by the SNMP agent. This object functions like an alarm-cutoff switch in the central office. Note that the object has no effect on alarm monitoring and logging, or the generation of SNMP notifications and syslog messages.
- ceAlarmNotifiesEnable—The severity level of alarms that cause an SNMP ceAlarmAsserted or ceAlarmCleared notification to be generated.
- ceAlarmSyslogEnable—The severity level of alarms that cause a syslog message to be generated.

**Note** See the "Enabling Traps and Syslog Messages for Alarms" section on page A-16 for more information on how to use ceAlarmNotifiesEnable and ceAlarmSyslogEnable.

## Interpreting Alarm Information in the CISCO-ENTITY-ALARM-MIB

To obtain information about router alarms from the CISCO-ENTITY-ALARM-MIB, do the following:

**Step 1** To determine if any alarms are currently being asserted on the router, read the values of the objects in ceAlarmTable. Each entry in the table contains information about the alarms currently being asserted by each physical entity. Each entry is indexed by the entPhysicalIndex (ENTITY-MIB) of the entity.

**Step 2** To obtain information about individual alarms, read the values of the ceAlarmDescrSeverity and ceAlarmDescrText objects. See Figure A-7 for an illustration of how to determine the entity that each alarm is associated with.

**Step 3** To determine the total number of alarms currently being asserted (by all entities), read the values of ceAlarmCriticalCount, ceAlarmMajorCount, and ceAlarmMinorCount.

## CISCO-ENTITY-ALARM-MIB Examples

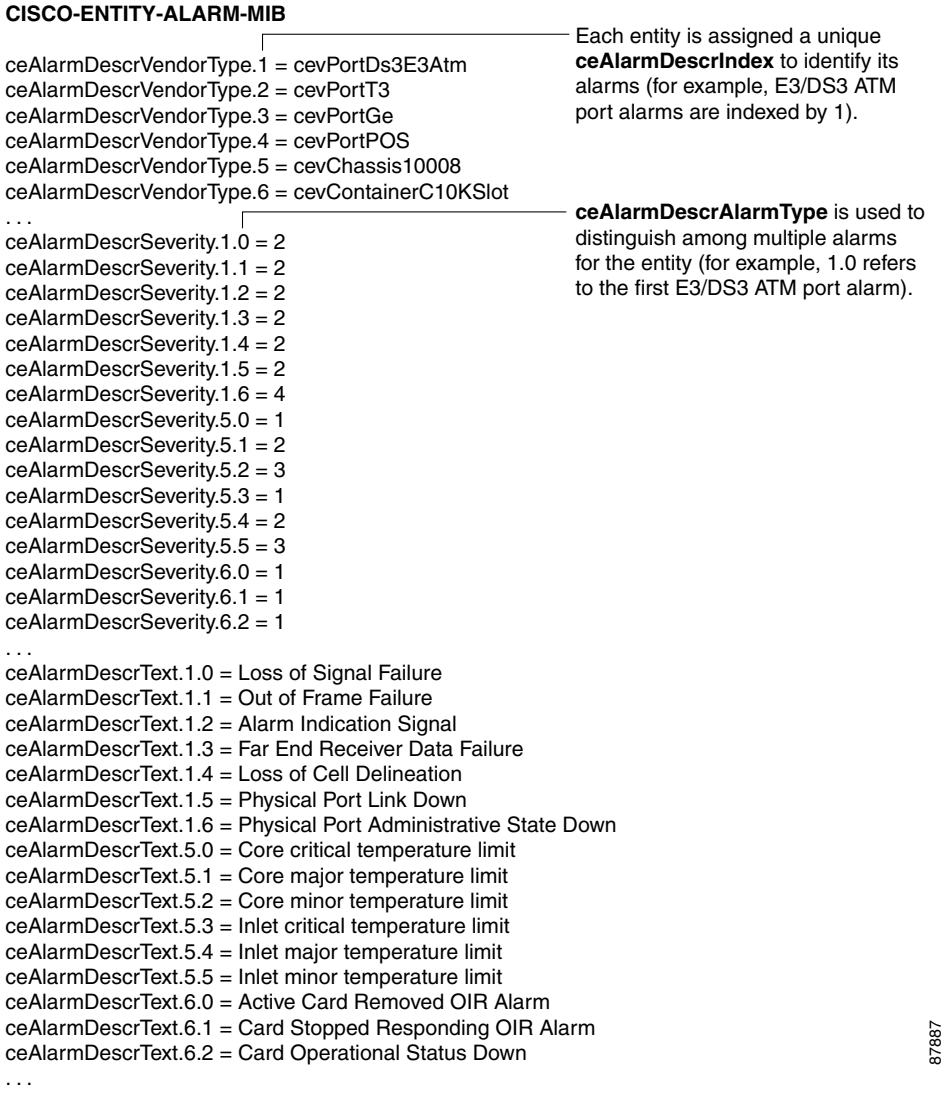
The following is an example of information in the CISCO-ENTITY-ALARM-MIB:

```
ceAlarmDescrVendorType.1 = cevPortDs3E3Atm
ceAlarmDescrVendorType.2 = cevPortT3
ceAlarmDescrVendorType.3 = cevPortGe
ceAlarmDescrVendorType.4 = cevPortPOS
ceAlarmDescrVendorType.5 = cevChassis10008
ceAlarmDescrVendorType.6 = cevContainerC10KSlot
ceAlarmDescrVendorType.7 = cevContainerC10KFanTraySlot
ceAlarmDescrVendorType.8 = cevPowerSupplyC10KAC
ceAlarmDescrVendorType.9 = cevFanTrayC10008
ceAlarmDescrVendorType.10 = cevCpuCreRp
ceAlarmDescrVendorType.11 = cevPortFEIP
ceAlarmDescrVendorType.12 = cevPortOC3SUNI
```

```
ceAlarmDescrVendorType.13 = cevPortOC12SUNI
ceAlarmDescrVendorType.14 = cevPortChOc3Stm1
ceAlarmDescrVendorType.15 = cevPortChOc12
ceAlarmDescrVendorType.16 = cevPortChE1T1
ceAlarmDescrSeverity.1.0 = 2
ceAlarmDescrSeverity.1.1 = 2
ceAlarmDescrSeverity.1.2 = 2
ceAlarmDescrSeverity.1.3 = 2
ceAlarmDescrSeverity.1.4 = 2
ceAlarmDescrSeverity.1.5 = 2
ceAlarmDescrSeverity.1.6 = 4
ceAlarmDescrSeverity.2.0 = 2
ceAlarmDescrSeverity.2.1 = 2
ceAlarmDescrSeverity.2.2 = 2
ceAlarmDescrSeverity.2.3 = 2
ceAlarmDescrSeverity.2.4 = 2
ceAlarmDescrSeverity.2.5 = 2
ceAlarmDescrSeverity.2.6 = 2
ceAlarmDescrSeverity.2.7 = 2
ceAlarmDescrSeverity.2.8 = 2
ceAlarmDescrSeverity.2.9 = 2
ceAlarmDescrSeverity.2.10 = 4
ceAlarmDescrSeverity.3.0 = 1
ceAlarmDescrSeverity.3.1 = 1
. . .
ceAlarmDescrText.1.0 = Loss of Signal Failure
ceAlarmDescrText.1.1 = Out of Frame Failure
ceAlarmDescrText.1.2 = Alarm Indication Signal
ceAlarmDescrText.1.3 = Far End Receiver Data Failure
ceAlarmDescrText.1.4 = Loss of Cell Delineation
ceAlarmDescrText.1.5 = Physical Port Link Down
ceAlarmDescrText.1.6 = Physical Port Administrative State Down
ceAlarmDescrText.2.0 = Far End Remote Alarm Indication Alarm
ceAlarmDescrText.2.1 = Near End Remote Alarm Indication Alarm
ceAlarmDescrText.2.2 = Far End Alarm Indication Signal
ceAlarmDescrText.2.3 = Near End Alarm Indication Signal
ceAlarmDescrText.2.4 = Far End Loss of Frame Failure
ceAlarmDescrText.2.5 = Far End Loss of Signal Failure
ceAlarmDescrText.2.6 = Far End Test Code
ceAlarmDescrText.2.7 = Far End Idle
ceAlarmDescrText.2.8 = Other Failure
ceAlarmDescrText.2.9 = Physical Port Link Down
ceAlarmDescrText.2.10 = Physical Port Administrative State Down
ceAlarmDescrText.3.0 = Physical Port Link Down
ceAlarmDescrText.3.1 = C10K Gigabit Ethernet GBIC missing
. . .
```

Figure A-7 shows how indexes are used to distinguish router alarms.

*Figure A-7 CISCO-ENTITY-ALARM-MIB Indexes*




The sample CISCO-ENTITY-ALARM-MIB shown above contains the following alarm information (note that only portions of the MIB are shown):

| Index | Alarm Text | Severity | Component |
|---|---|---|---|
| 1.0 | Loss of Signal Failure | 2 | E3/DS3 ATM port |
| 1.5 | Physical Port Link Down | 2 | E3/DS3 ATM port |
| 5.0 | Core critical temperature limit | 1 | C10008 Chassis |
| 5.5 | Inlet minor temperature limit | 3 | C10008 Chassis |
| 6.0 | Active Card Removed OIR Alarm | 1 | Chassis slot |
| 6.2 | Card Operational Status Down | 1 | Chassis slot |

# Enabling Traps and Syslog Messages for Alarms

By default, SNMP generates a trap and a syslog message when an alarm is asserted or cleared. You can, however, control the type of alarms for which traps and syslog messages are generated, or disable the traps and messages completely, by performing the instructions in the following sections.

### Enabling Traps for Alarms

To enable or disable SNMP traps for alarms, do either of the following. By default, SNMP generates a trap when an alarm is asserted or cleared.

- At the CLI, enter the following command. Use the **no** form of the command to disable the traps.

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

- Through SNMP, set the following CISCO-ENTITY-ALARM-MIB object:

  ceAlarmNotifiesEnable—The severity level of alarms that cause an SNMP trap to be generated: critical(1), major(2), minor(3), or info(4). Disable traps by setting ceAlarmNotifiesEnable to 0.

  For example, set ceAlarmNotifiesEnable to major to generate a trap for major and critical alarms; or, set ceAlarmNotifiesEnable to minor to generate a trap for minor, major, and critical alarms. See the "Viewing Active Alarms Through the CLI" section on page A-12 for descriptions of alarm severities.

**Note** The CISCO-ENTITY-ALARM-MIB monitors alarms only for physical entities defined in the ENTITY-MIB entPhysicalTable. Alarms for logical entities, such as channelized interfaces, are monitored by Cisco IOS software through syslog.

### Enabling Syslog Messages for Alarms

By default, the router logs a syslog message each time an alarm is asserted or cleared. You can, however, use the following CISCO-SYSLOG-MIB object to configure the types of alarms for which a syslog message is generated:

- ceAlarmSyslogEnable—The severity level of alarms to generate a syslog message for: critical(1), major(2), minor(3), or info(4). See the "Viewing Active Alarms Through the CLI" section on page A-12 for descriptions of alarm severities. To disable these syslog messages, set ceAlarmSyslogEnable to 0.

In addition, the following CISCO-SYSLOG-MIB objects provide SNMP notification when syslog messages are logged in response to alarms:

- clogNotificationsEnabled—Specifies whether to generate a notification when a syslog message is logged. Set this object to true(1) to enable the notifications, or false(2) to disable them.
- clogMessageGenerated—SNMP notification sent when a syslog message is generated.

# 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 Traps

To determine if an interface has failed, you can monitor linkDown and linkUp traps for the interface. See the "Enabling Interface linkUp/linkDown Traps" section on page A-17 for instructions on how to enable these traps.

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

### Check the Interface for Alarms

You can also check to see if an interface is currently asserting either of the following alarms, which indicate that the interface is down and can not send or receive traffic:

- Physical Port Link Down—Indicates that the operational state of an interface is Down.
  - For Ethernet, OC-*x*, OC-*x* ATM, OC-*x* POS, and STM-*x* line cards, the alarm has a severity level of critical(1).
  - For line cards that support serial lines (for example, E1/T1, T3, and E3/DS3 ATM), the alarm has a severity level of major(2) or minor(3).
- Physical Port Administrative State Down—Indicates that the administrative (desired) state of an interface is Down. When the administrative state is Down, the operational state also changes to Down.
  - For all line cards, this alarm is severity level info(4).

For information about how to monitor alarms, see the "Using Alarms to Monitor Outages" section on page A-11. Also see the "Using the CISCO-ENTITY-ALARM-MIB to Monitor Alarms" section and the "Interpreting Alarm Information in the CISCO-ENTITY-ALARM-MIB" section on page A-13.

**Note** SNMP generates a ceAlarmAsserted or ceAlarmCleared trap when an alarm is generated or cleared. You can read the CISCO-ENTITY-ALARM-MIB to see if any interfaces are asserting alarms.

## Enabling Interface linkUp/linkDown Traps

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 traps:

**Step 1** Issue the following CLI command to enable linkUp and linkDown traps 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 traps are enabled or disabled for that interface.

**Step 3** To enable linkUp and linkDown traps on an interface, set ifLinkUpDownTrapEnable to enabled(1). For information about how to configure the router to send linkDown traps only for the lowest layer of an interface, see the "SNMP Trap Filtering for linkDown Traps" section on page A-18.

**Note** Some interface layers do not support linkDown traps (for example, some ATM layers).

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

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

**Step 5** To enable linkUp and linkDown traps on ATM subinterfaces, issue the following command:

```
Router(config)# snmp-server enable traps atm subif
```

**Step 6** To enable linkUp and linkDown traps on an ATM permanent virtual circuit (PVC), issue the following commands. In the first command, **interval** specifies the minimum interval between successive traps, and **fail-interval** specifies the minimum interval for storing failed time stamps.

```
Router(config)# snmp-server enable traps atm pvc interval seconds fail-interval seconds
Router(config)# interface atm slot/subslot/port
Router(config-if)# pvc vpi/vci
Router(config-if-atm-vc)# oam-pvc manage
```

**Step 7** To disable traps, use the **no** form of the appropriate command.

## SNMP Trap Filtering for linkDown Traps

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

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

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

# Monitoring PXF Utilization

This section describes how to use SNMP to monitor parallel express forwarding network processor (PXF) utilization on the router by:

- Determining PXF Utilization and Efficiency
- Monitoring PXF Performance Thresholds and Restarts

### Purpose and Benefits

The CISCO-ENTITY-PFE-MIB provides SNMP access to performance information for the packet forwarding engine (PFE), which accelerates certain IP features in order to improve network performance. The MIB contains objects to monitor PFE utilization and efficiency. On the Cisco 10000 series ESR, the PFE is the parallel express forwarding network processor (PXF), which is part of the performance routing engine (PRE).

The MIB provides the following benefits:

- Summarizes the PXF utilization and efficiency information in the following CLI command:

  ```
  show hardware pxf cpu context
  ```

- Provides information about performance trends for 1-minute, 5-minute, and 15-minute intervals
- Maintains a 24-hour history of PXF utilization and efficiency
- Measures PXF performance against user-configurable utilization and efficiency thresholds and generates an event when a threshold is exceeded or the PXF is restarted

### MIBs Used to Monitor PXF Utilization

- CISCO-ENTITY-PFE-MIB

## Determining PXF Utilization and Efficiency

CISCO-ENTITY-PFE-MIB utilization and efficiency objects are used to measure PXF performance:

- PXF *utilization* is the percentage of the PXF currently being used for processing. As PXF processing increases, utilization rises from 0 to 100 percent.
- PXF *efficiency* measures how well the PXF is performing. The higher the value, the greater the PXF's efficiency. During normal operating conditions, PXF efficiency is typically 100 percent. As efficiency degrades, this value decreases.

To determine PXF utilization and efficiency on the router, view the information in the following MIB tables:

- cePfePerfCurrentTable—Utilization and efficiency percentages: current, 1-minute, and 5-minute.
- cePfePerfIntervalTable—Performance statistics for the past 24 hours, in 15-minute intervals. The table holds 96 measurement intervals, less if the PXF has not been running for 24 hours.

  The start of each 15-minute interval is based on the time that the PXF was last started or restarted, which may not match the start of a quarter-hour increment in real time (for example, 10:45 or 11:15). For example, if the PXF was started at 10:20, subsequent 15-minute intervals start at 10:35, 10:50, and so on.
- cePfePerfTotalTable—Utilization and efficiency for the past 24 hours.

## Monitoring PXF Performance Thresholds and Restarts

You can use the CISCO-ENTITY-PFE-MIB to set thresholds for PXF utilization and efficiency, and monitor PXF performance against those thresholds. SNMP compares PXF performance (ceCpfePerfCurrentTable) to the thresholds (cePfePerfConfigTable) and generates an event when PXF utilization or efficiency reaches or exceeds a threshold. You can log the event to an event history table (cePfeHistTable), generate an SNMP notification, do both, or take no action. A PXF event is also generated each time the PXF is restarted.

For example, if the PXF 1-minute utilization measurement (cePfePerfCurrent1MinUtilization) reaches or exceeds its threshold (cePfePerfThld1MinUtilization), SNMP generates a thld1MinUtilizationEvent. See the MIB object HistEventType for descriptions of events.

Perform the following steps to track PXF utilization and efficiency by setting and monitoring PXF thresholds:

**Step 1** Use cePfePerfConfigTable to define acceptable thresholds for PXF utilization and efficiency.

**Step 2** Set cePfeHistNotifiesEnable to one of the following values to specify what SNMP should do when a threshold is exceeded or the PXF is restarted:

- none(1)—SNMP takes no action. This is the default.
- log(2)—Create an entry in the cePfeHistTable.
- notify(3)—Send an SNMP notification.
- logAndNotify(4)—Create a cePfeHistTable entry and send an SNMP notification.

**Step 3** To log events to cePfeHistTable, use cePfeHistTableSize to specify the maximum number of entries to allow in the table. When the table becomes full, each new event overwrites the oldest entry in the table.

**Step 4** If you set cePfeHistNotifiesEnable to log(2) or logAndNotify(4), you can view the cePfeHistTable for information about exceeded thresholds and PXF restarts.

# Preprovisioning Line Cards

This section provides information about the process of preprovisioning line cards and its affect on SNMP data. The preprovisioning feature preconfigures a line card slot for a particular type of line card before the line card is actually inserted into the chassis. The system adds a basic configuration for the line card to the system's running configuration file, and then applies this configuration to the line card when it is actually inserted in the chassis.

**Note** You cannot use SNMP to preprovision a line card slot. You must use the CLI **card** command to do that. For instructions, see the *Cisco 10000 Series Router Line Card Slot Preprovisioning* feature description under the Cisco 10000 Series Router New Features documentation link on CCO.

## Installing a Preprovisioned Line Card

When a line card is inserted in the Cisco 10000 chassis, the following occurs:

- If the inserted line card matches the type of line card preprovisioned for the slot, the system applies the preprovisioned configuration to the line card.
- If the line card slot was not preprovisioned, the system applies a basic configuration to the line card and adds that configuration to the running configuration file.
- If the line card slot was preprovisioned for one type of line card, but another type of line card was inserted, the system replaces the preprovisioned configuration (in the running configuration file) with a basic configuration for the line card that was actually inserted.

To find out the type of card that a slot is configured to use, enter the **show running-config** command.

### Affected MIBs

The information in the following MIB tables is affected when a preprovisioned line card is inserted into the Cisco 10000 chassis, or you enter CLI commands that affect line card operation:

- ENTITY-MIB (entPhysicalTable and entAliasMappingTable)
- CISCO-ENTITY-ASSET-MIB (ceAssetTable)
- CISCO-ENTITY-FRU-CONTROL-MIB (cefcModuleTable)

# Replacing Line Cards—MIB State Characteristics

When you replace a line card in the Cisco 10000 chassis, the contents of MIBs are affected as follows. If you replace a line card with:

- Another type of line card (for example, if you replace a Gigabit Ethernet line card with a channelized T3 line card), the original line card information is removed from the MIBs.
- Another line card of the *same* type, the MIBs retain the original line card configuration. This enables you to replace a line card without losing its configuration. For example, if you replace a Gigabit Ethernet line card that has 50 subinterfaces, the MIBs retain the information about the line card and its subinterfaces. To replace the original line card information in the MIBs, see the following steps.

To replace a line card with another line card of the same type and remove the original line card information from the MIBs, perform the following steps:

**Step 1** To shut down the line card, issue the following CLI command (where *slot_number* is 1 through 8):

```
hw-module slot slot_number shutdown
```

**Step 2** Wait 30 seconds for the line card failure LED to light.

**Step 3** Remove the line card from the chassis.

**Note** If you do not plan to install another line card in the slot for some period of time, we recommend that you issue the **no card** command (see Step 4).

**Step 4** To remove line card information from the router configuration and MIBs, issue the following CLI command. For example, the command **no card 5/0** removes configuration information for the line card in slot 5.

```
no card slot/subslot
```

**Step 5** (Optional) To verify that the line card configuration information was removed from the MIBs, view the contents of the MIBs.

**Step 6** Insert a new line card in the chassis slot.

**Step 7** To activate the newly installed line card, issue the following CLI command:

```
no hw-module slot slot_number shutdown
```

# Performing Bulk-File Retrieval

This section describes how to use SNMP to perform bulk retrieval of large amounts of data from the router. You can use this feature to transfer information between the SNMP agent and manager (such as QoS statistics, interface statistics, and entPhysicalTable entries).

### Purpose and Benefits

In previous releases, a management application was required to enter lengthy sequences of SNMP **get-next** or **get-bulk** requests to retrieve large amounts of data from the router.

The SNMP bulk-file retrieval feature simplifies this process, and may result in better performance. To perform a bulk-file retrieval:

1. Define the characteristics of the bulk file.
2. Specify the data to include in the bulk file.
3. Create the bulk file and fill it with the data you want to transfer.
4. Use the File Transfer Protocol (FTP) utility to copy the bulk file from the router to another system.

To perform the bulk-file retrieval, either:

- Enter SNMP **set** and **get** requests from the host (see the "SNMP Commands" section on page A-23 for command examples).
- Create a management application that issues SNMP **set** and **get** requests.

The MIB enhancements feature also includes a Java applet that retrieves the router's ifTable using the bulk-retrieval process (see the "Java Applet" section on page A-25).

### MIBs Used for Bulk-File Retrieval

- CISCO-BULK-FILE-MIB
- CISCO-FTP-CLIENT-MIB

## Bulk-File Retrieval Processing Steps

This section describes how to perform a bulk-file retrieval. For examples of this process, see the "SNMP Commands" section on page A-23 and the "Java Applet" section on page A-25. For detailed information about MIB objects, their characteristics, and valid values, see the MIB.

**Step 1** Define the characteristics of a bulk file by creating a row in the CISCO-BULK-FILE-MIB cbfDefineFileTable:

a. Determine a unique index to assign to the row.

b. Set cbfDefineFileTable objects:

cbfDefineFileEntryStatus = createAndGo(4) or createAndWait(5)
cbfDefineFileName = *bulk_file_name*
cbfDefineFileStorage = ephemeral(1)
cbfDefineFileFormat = bulkASCII(3)

**Step 2** Define the data to include in the bulk file by creating a row in cbfDefineObjectTable:

a. Determine a unique index to assign to the row.

b. Set cbfDefineObjectTable objects:

cbfDefineFileObjectStatus = createAndGo(4) or createAndWait(5)
cbfDefineObjectID = *the OID of the object instance or table column*
cbfDefineObjectClass = object(1) or lexicaltable(2)

**c.** (Optional) To include specific table rows in the bulk file, set the following MIB objects. To use this option, you must set cbfDefineObjectClass = lexicaltable(2).

cbfDefineObjectTableInstance = *starting table row*
cbfDefineObjectNumEntries = *number of table rows to include*

For example, to include rows 2 through 12 of ifTable, set cbfDefineObjectTableInstance = ifTable.2 and cbfDefineObjectNumEntries = 10.

**Step 3** Create the bulk file, fill it with data, and check its status:

**a.** Set cbfDefineFileNow = create(3).

**b.** Perform a **get-next** on cbfStatusFileState, using the bulk file's cbfDefineFileIndex.

**c.** Do not take any action until cbfStatusFileState = ready(2).

**Step 4** Configure FTP to copy the bulk file to an FTP server by creating a row in the CISCO-FTP-CLIENT-MIB cfcRequestTable:

**a.** Determine a unique index to use for the row.

**b.** Set cfcRequestTable objects:

cbfRequestEntryStatus = createAndWait(5) or createAndGo(4)
cfcRequestOperation = putASCII(2)
cfcRequestLocalFile = *name of the bulk file on the router*
cfcRequestRemoteFile = *name (and path) to copy bulk file to on destination FTP server*
cfcRequestServer = *IP address or fully qualified name of FTP server*
cfcRequestUser = *a valid user name for FTP server*
cfcRequestPassword = *password for FTP user name*

**c.** Set cfcRequestEntryStatus to active(1) to activate the row, which starts the bulk-file transfer.

**d.** Check cfcRequestResult to view the result of the FTP operation.

## SNMP Commands

Figure A-1 shows sample SNMP commands for performing bulk-file retrieval. These commands are samples only; your commands will be different. Check the MIB for valid values. The numbers in the figure correspond to the steps in the "Bulk-File Retrieval Processing Steps" section on page A-22. Notes and background information appear in Table A-1.

**Note** This example makes use of the SNMP EMANATE tool (from SNMP Research International). In the following commands, *rtr_IP_addr* is the IP address of the router.

*Figure A-1 Sample SNMP Command for Bulk-File Retrieval*

```
1  setany -v2c rtr_IP_addr private cbfDefineFileEntryStatus.1 -i 4
   setany -v2c rtr_IP_addr private cbfDefineFileName.1 -D "QoSstats"
   setany -v2c rtr_IP_addr private cbfDefineFileStorage.1 -i 1
   setany -v2c rtr_IP_addr private cbfDefineFileFormat.1 -i 3

2  setany -v2c rtr_IP_addr private cbfDefineObjectEntryStatus.1.3 -i 4
   setany -v2c rtr_IP_addr private cbfDefineObjectID.1.3 -d 1.3.6.1.2.1.4.20
   setany -v2c rtr_IP_addr private cbfDefineObjectClass.1.3 -i 2

3  setany -v2c rtr_IP_addr private cbfDefineFileNow.1 -i 3
   getone -v2c rtr_IP_addr private cbfStatusFileState.1.1

4  setany -v2c rtr_IP_addr private cfcRequestEntryStatus.1 -i 5
   setany -v2c rtr_IP_addr private cfcRequestOperation.1 -i 2
   setany -v2c rtr_IP_addr private cfcRequestLocalFile.1 -D "QoSstats"
   setany -v2c rtr_IP_addr private cfcRequestRemoteFile.1 -D "C10kQoS"
   setany -v2c rtr_IP_addr private cfcRequestServer.1 -D "stats.cisco.com"
   setany -v2c rtr_IP_addr private cfcRequestUser.1 -D "JoeSmith"
   setany -v2c rtr_IP_addr private cfcRequestPassword.1 -D "bluefi$h"
   setany -v2c rtr_IP_addr private cfcRequestEntryStatus.1 -i 1
```

69731

**Step 1** A row is created for a bulk file named QoSstats and the row is placed in the Active state.

An index of 1 is assigned to the row and used to access table objects for the row (for example, cbfDefineFileEntryStatus**.1**, cbfDefineFileName**.1**, cbfDefineFileStorage**.1**, and so on).

The bulk file stores data only until it is read, and its format is human-readable ASCII.

**Step 2** A row is created and its index is **.1.3** (cbfDefine**File**Index and cbfDefine**Object**Index).

The MIB settings specify that data in the ipAddrTable is to be included in the bulk file.

**Step 3** The bulk file is created, and cbfDefineFileIndex is used to check that the bulk file was created.

**Step 4** The commands set up an FTP **put** request to copy the bulk file (QoSstats) to the stats.cisco.com server to a file named C10kQoS. By default, the file is copied to the specified user's home directory; however, you can specify another directory. For example, cfcRequestRemoteFile = /C10Kstats/QoSstats copies the bulk file to the directory /C10Kstats.

If you use SNMP commands, consider the following:

- For each row in a table, you must determine a unique index to use to access table objects for the row. The index must be unique among all rows in the table. You must define the index when you create the row.
- To create a row in a table:
  - Append the row's index to the table's *xxxEntryStatus* object
  - Set *xxxEntryStatus* = createAndGo(4) or createAndWait(5)

  The system creates the row and assigns the specified index to the row. For example, the following command creates a row in cbfDefineFileTable and sets the row to the Inactive state. The row is assigned an index of 1.

  ```
  setany -v2c rtr_IP_addr private cbfDefineFileEntryStatus.1 -i 5
  ```

  Use this index value to access the row's other MIB objects (for example, cbfDefineFileName.1, cbfDefineFileStorage.1, and so on).

## Java Applet

To use the Java applet to perform a bulk-file retrieval of the ifTable, follow these steps:

1. Make sure the router is connected to a workstation that supports the Java 2 platform (which is required to run the applet).
2. Go to the Cisco FTP site at the following URL:

   ftp://ftp-eng.cisco.com/auto/ftp/omega/cheops
3. Copy the following file from the FTP site to your workstation:

   10kApplets.jar
4. At the workstation, enter the following command to launch the applet. (Note that applet.BulkFileRetrieval tells the system to run the bulk-file retrieval class or program within the JAR file.)

   ```
   java -cp <JAR_file_location> applet.BulkFileRetrieval
   ```
5. Enter the following information in the window that is displayed:
   - IP address of the Ethernet port on the router
   - SNMP version and community
   - IP address of the destination FTP server to transfer the bulk file to
   - A valid username and password for the server
   - Home directory of the specified user (the bulk file is copied here)
6. Click **Retrieve BULK-FILE** to start the bulk-file retrieval.

   The system copies the ifTable to a bulk file named ifTable–bulkFile<*MonthDay–HourMinSec*> (for example, ifTable–bulkFileJan3–17hr9min16sec), then copies the bulk file to the home directory of the specified user on the destination FTP server.
7. Click the **BULK-FILE Data** tab to view the bulk file.

Figure A-2 shows the Java applet for performing a bulk-file retrieval. Numbers correspond to steps in the "Bulk-File Retrieval Processing Steps" section on page A-22. See Table 0-1 for background information about certain steps in the applet.

*Figure A-2 Java Applet for Bulk-File Retrieval*

```
public int createCbfDefineFileRow(String bulkFileName) {

(1a) int[] cbfDefineFileTableIndex = {getRandomNumber()};
     String indexValue = snmp.makeOIDFromArray(cbfDefineFileTableIndex);

(1b) snmp.snmpSet_addVarbind("cbfDefineFileEntryStatus",
                             indexValue,
                             RowStatusEnum_createAndGo);

     snmp.snmpSet_addVarbind("cbfDefineFileName",
                             indexValue,
                             bulkFileName);

     snmp.snmpSet_addVarbind("cbfDefineFileStorage",
                             indexValue,
                             FileStorageEnum_ephemeral);

     snmp.snmpSet_addVarbind("cbfDefineFileFormat",
                             indexValue,
                             FileFormatEnum_bulkASCII);

     snmp.snmpSet_go();
}


public boolean createCbfDefineObjectRow(int bulkFileId,
                                        String objectClass,
                                        String objectId) {

(2a) int[] cbfDefineObjectTableIndex = {bulkFileId, getRandomNumber()};
     String indexValue = snmp.makeOIDFromArray(cbfDefineObjectTableIndex);

(2b) snmp.snmpSet_addVarbind("cbfDefineObjectEntryStatus",
                             indexValue,
                             RowStatusEnum_createAndGo);

     snmp.snmpSet_addVarbind("cbfDefineObjectClass", indexValue, objectClass);

     snmp.snmpSet_addVarbind("cbfDefineObjectID", indexValue, objectId);

     snmp.snmpSet_go();
     }


     public boolean startAndMonitorBulkFileCreation(int bulkFileId) {

(3a)      String indexValue = "." + bulkFileId;
          snmp.snmpSet_addVarbind("cbfDefineFileNow",
                                  indexValue,
                                  FileNowEnum_create);
          snmp.snmpSet_go();

(3b)      SnmpVarBind result = snmp.snmpGetNextObject("cbfStatusFileState", indexValue);
          String fileStateIndex = snmp.extractIndexValues(result);
          int fileStateValue = result.getValue()
```

69732

*Figure A-3 Java Applet for Bulk-File Retrieval (continued)*

```
3c  while (fileStateValue == FileStateEnum_running) {
              sleep(FileStatePollInterval);
              result = snmp.snmpGetObject("cbfStatusFileState", fileStateIndex);
              fileStateValue = result.getValue();
         }

         boolean returnResult = determineResult(fileStateValue);
         return returnResult;
    }


    public boolean startAndMonitorBulkFileTransfer(String bulkFileName,
         String     bulkFileType,
         String     ftpServerAddr,
         String     ftpServerUsername,
         String     ftpServerPassword) {

4a       int[] cfcRequestTableIndex = {getRandomNumber()};
         String indexValue = snmp.makeOIDFromArray(cfcRequestTableIndex);

4b       snmp.snmpSet_addVarbind("cfcRequestEntryStatus",
                                 indexValue,
                                 RowStatusEnum_createAndWait);

         snmp.snmpSet_addVarbind("cfcRequestOperation",
                                 indexValue,
                                 bulkFileType);

         snmp.snmpSet_addVarbind("cfcRequestLocalFile",
                                 indexValue,
                                 bulkFileName);

         snmp.snmpSet_addVarbind("cfcRequestRemoteFile",
                                 indexValue,
                                 bulkFileName);

         snmp.snmpSet_addVarbind("cfcRequestServer",
                                 indexValue,
                                 ftpServerAddr);

         snmp.snmpSet_addVarbind("cfcRequestUser",
                                 indexValue,
                                 bulkFileUsername);

         snmp.snmpSet_addVarbind("cfcRequestPassword",
                                 indexValue,
                                 ftpServerPassword);

         snmp. snmpSet_go();
```

69733

*Figure A-4 Java Applet for Bulk-File Retrieval (continued)*

```
4c  snmp.snmpSet_addVarbind("cfcRequestEntryStatus",
                                indexValue,
                                RowStatusEnum_active);

        returnStatus = snmp.snmpSet_go();

4d      SnmpVarBind result = snmp.snmpGetObject("cfcRequestResult", indexValue);
        int requestResultState = result.getValue();
        int timeToCompletion = 0;
        while (requestResultState == cfcRequestResult_pending ||
                       timeToCompletion < BulkFileTransferTimeout) {
                  sleep(cfcRequestStatePollInterval);
                  timeToCompletion+=cfcRequestStatePollInterval;
                  result = snmp.snmpGetObject("cfcRequestResult", indexValue);
                  requestResultState = result.getValue();
        }

        boolean returnResult = determineResult(fileStateValue);
        return returnResult;
    }
```

69734

| | |
|---|---|
| **Step 1a** | Generate a random number to use as the index. |
| **Step 1b** | MIB objects are set as follows:<br>cbfDefineFileStorage = ephemeral(1)<br>cbfDefineFileFormat = bulkASCII(3) |
| **Step 2a** | Generate a random number to use as the index. |
| **Step 3b** | Use cbfDefineFileIndex to access cbfStatusFileState. |
| **Step 4c** | Poll cbfStatusFileState until the state changes from running(1) to ready(2). |
| **Step 5d** | Poll cfcRequestResult until the bulk-file transfer is no longer pending. |

# Monitoring Quality of Service

This section provides an example of how to use SNMP to access QoS configuration information and statistics on the router. It contains the following sections:



### Purpose and Benefits

Previously, the only way to access QoS configuration information and statistics was to enter **show** commands at the CLI.

With the enhanced management feature, you can use SNMP to access QoS configuration information and statistics on the router. This means that you can now collect and store QoS information for use in management applications. You can also use bulk-file transfer to copy the information to another system.

### MIBs Used for QoS

- CISCO-CLASS-BASED-QOS-MIB

# Configuring QoS

You configure QoS through the command line interface (CLI). For instructions, see the *Cisco 10000 Series Router Software Configuration Guide*, "Configuring Quality of Service."

# Accessing QoS Configuration Information and Statistics

The CISCO-CLASS-BASED-QOS-MIB provides access to QoS configuration information and statistics. Although you cannot use SNMP to configure QoS on the router, you can use SNMP to access QoS configuration information that has been configured through the CLI.

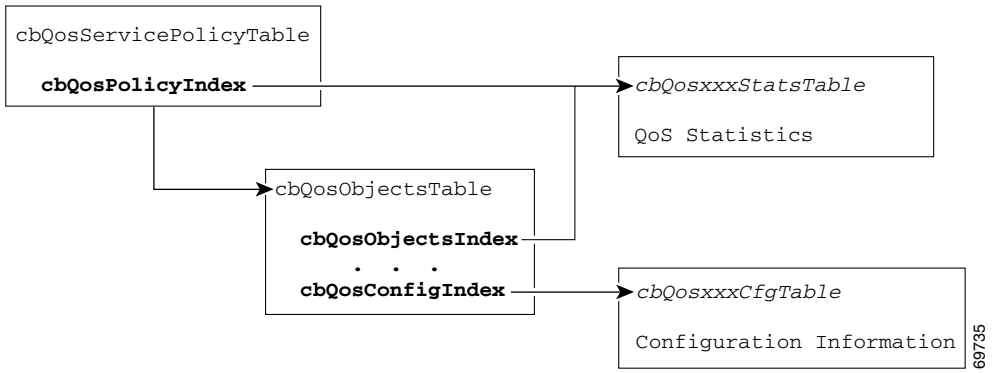
## QoS Indexes

The indexes for accessing QoS configuration information and QoS statistics are:

- cbQosPolicyIndex—System-assigned index that identifies a policy map attached to an interface. (When attached to an interface, a policy map is known as a *service policy*.)
- cbQosObjectsIndex—System-assigned index that identifies each unique run-time instance of a QoS feature (for example, policy map, class map, match statement, and feature action).
- cbQosConfigIndex—System-assigned index that identifies each unique configuration of a QoS feature (for example, a class map or police action). Note that QoS objects with the same configuration share the same cbQosConfigIndex.
- cbQosREDValue—The IP precedence or IP differentiated services code point (DSCP) of a Weighted Random Early Detection (WRED) action. It is used as the index for configuration information and statistics for each RED class.

Figure A-5 shows how these indexes provide access to QoS configuration information and statistics.

***Figure A-5 Cisco 10000 Series Router QoS Indexes***



To access QoS configuration information and statistics for a particular QoS feature:

1. Look in cbQosServicePolicyTable and find the cbQosPolicyIndex assigned to the policy in which the feature is used.
2. Use cbQosPolicyIndex to access the cbQosObjectsTable, and find the cbQosObjectsIndex and cbQosConfigIndex assigned to the QoS feature.
   - Use cbQosConfigIndex to access configuration tables (cbQos*xxx*CfgTable) for information about the feature.
   - Use cbQosPolicyIndex and cbQosObjectsIndex to access QoS statistics tables (cbQos*xxx*StatsTable) for information about the QoS feature.

## Sample QoS Configuration Settings

This section contains figures that show how QoS configuration settings are stored in CISCO-CLASS-BASED-QOS-MIB tables:

- Figure A-6 shows the sample QoS configuration that the other figures are based on.
- Figure A-7 on page A-32 shows the service policy and objects table.
- Figure A-8 on page A-33 shows policy map, class map, and police action configuration information.
- Figure A-9 on page A-34 shows RED class configuration settings for an ATM interface.

The figures in this section show information grouped by QoS object; however, the actual output of an SNMP query might show QoS information similar to the following. This is only a partial display of all QoS information for the configuration in Figure A-6.

```
c10k# getmany -v3 10.86.0.94 test-user ciscoCBQosMIB

cbQosIfType.1047 = subInterface(2)
cbQosIfType.1052 = subInterface(2)
cbQosPolicyDirection.1047 = input(1)
cbQosPolicyDirection.1052 = output(2)
cbQosIfIndex.1047 = 36
cbQosIfIndex.1052 = 36
cbQosFrDLCI.1047 = 0
cbQosFrDLCI.1052 = 0
cbQosAtmVPI.1047 = 0
cbQosAtmVPI.1052 = 0
cbQosAtmVCI.1047 = 0
cbQosAtmVCI.1052 = 0
cbQosConfigIndex.1047.1047 = 1045
cbQosConfigIndex.1047.1048 = 1025
cbQosConfigIndex.1047.1050 = 1027
cbQosConfigIndex.1047.1051 = 1046
cbQosConfigIndex.1052.1052 = 1045
cbQosConfigIndex.1052.1053 = 1025
cbQosConfigIndex.1052.1055 = 1027
cbQosConfigIndex.1052.1056 = 1046
cbQosObjectsType.1047.1047 = policymap(1)
cbQosObjectsType.1047.1048 = classmap(2)
cbQosObjectsType.1047.1050 = matchStatement(3)
cbQosObjectsType.1047.1051 = police(7)
cbQosObjectsType.1052.1052 = policymap(1)
cbQosObjectsType.1052.1053 = classmap(2)
cbQosObjectsType.1052.1055 = matchStatement(3)
cbQosObjectsType.1052.1056 = police(7)
cbQosParentObjectsIndex.1047.1047 = 0
cbQosParentObjectsIndex.1047.1048 = 1047
cbQosParentObjectsIndex.1047.1050 = 1048
```

```
    cbQosParentObjectsIndex.1047.1051 = 1048
    cbQosParentObjectsIndex.1052.1052 = 0
    cbQosParentObjectsIndex.1052.1053 = 1052
    cbQosParentObjectsIndex.1052.1055 = 1053
    cbQosParentObjectsIndex.1052.1056 = 1053
    cbQosPolicyMapName.1045 = pm-1Meg
    cbQosPolicyMapDesc.1045 =
    cbQosCMName.1025 = class-default
    cbQosCMDesc.1025 =
    cbQosCMInfo.1025 = matchAny(3)
         . . .
```

***Figure A-6 GigabitEthernet QoS Configuration—CLI show Commands***

```
c10k# show class-map
 Class Map match-any class-default (id 0)
   Match any

 Class Map match-any cm1 (id2)
  Description: class map #1
   Match ip  dscp 48

c10k# show policy-map
  Policy Map pm1
    Class cm1
      shape 1200000
      random-detect dscp-based
      random-detect dscp 32 202 8000 20
      random-detect dscp 44 200 6000 22
      random-detect dscp 61 201 7000 22
  Policy Map pm-1Meg
    Class class-default
      police 1000000 8000 8000 conform-action transmit exceed-action drop

c10k# show policy-map interface
 GigabitEthernet1/0/0.1

  Service-policy input: pm-1Meg (1057)

    Class-map: class-default (match-any) (1058/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1060)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Police:
        1000000 bps, 8000 limit, 8000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop

  Service-policy output: pm-1Meg (1062)

    Class-map: class-default (match-any) (1063/0)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any  (1065)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Output queue: 0/8192; 0/0 packets/bytes output, 0 drops
      Police:
        1000000 bps, 8000 limit, 8000 extended limit
        conformed 0 packets,0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
```

69736

*Figure A-7 GigabitEthernet QoS—Service Policy and Objects Tables*

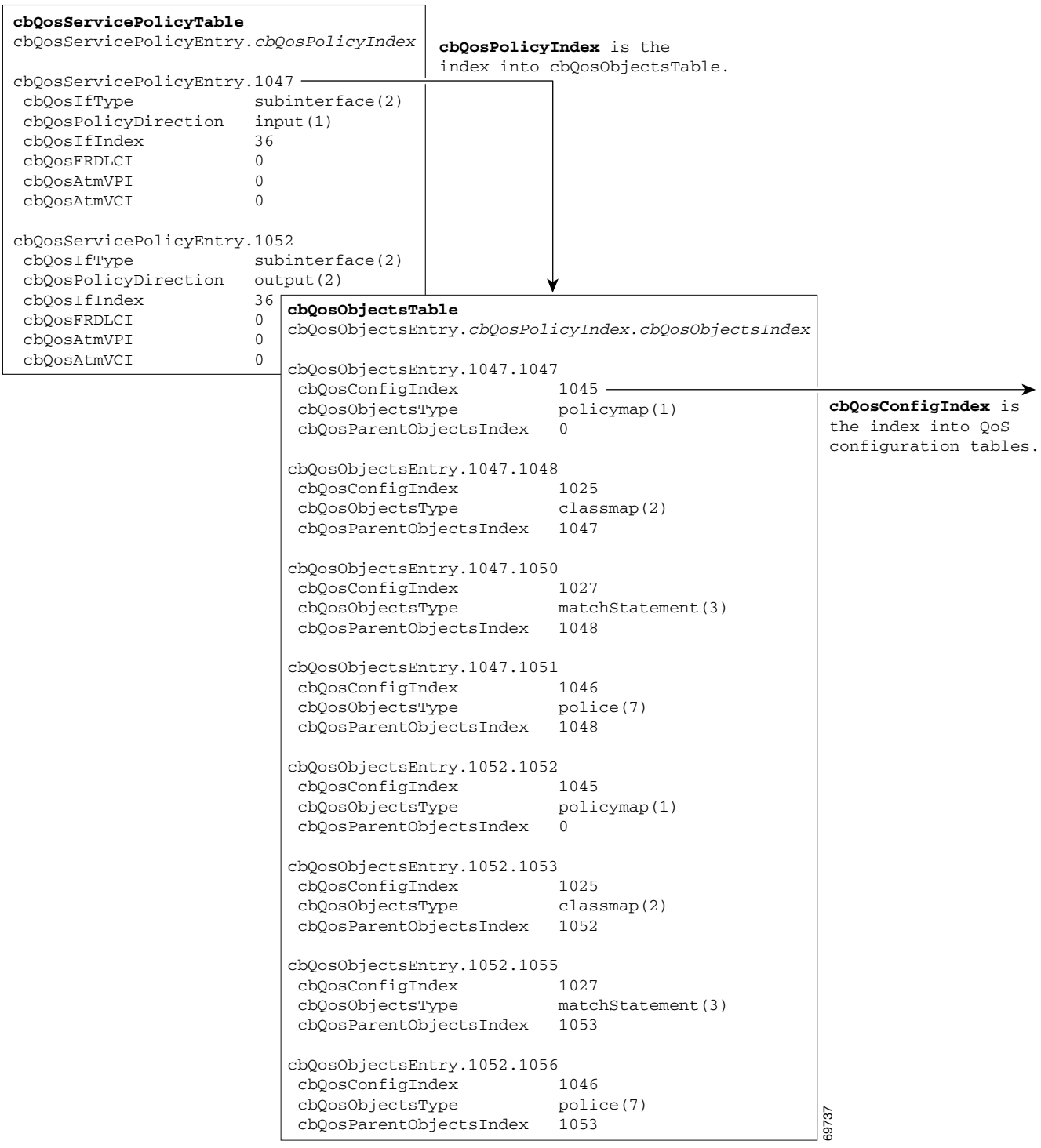


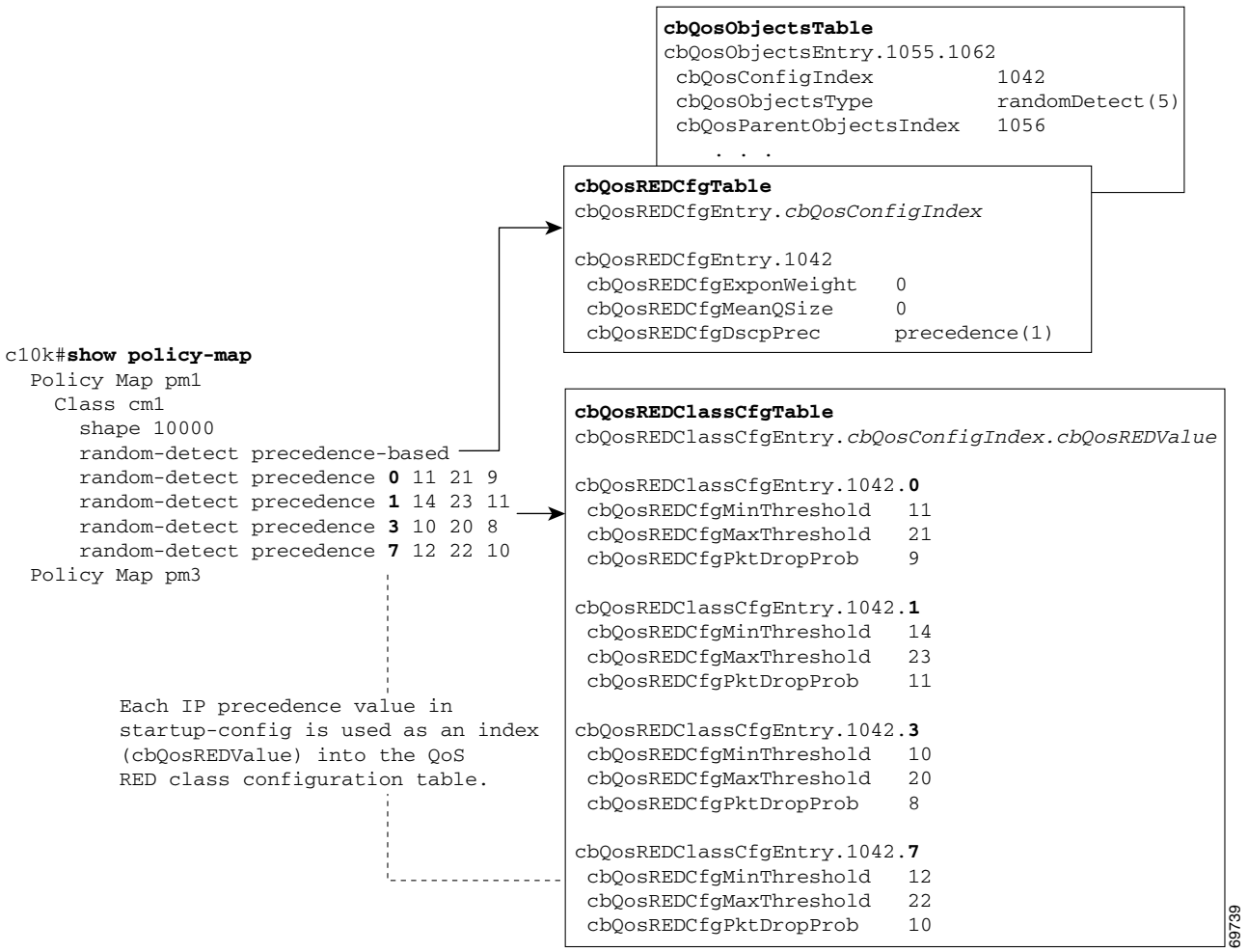
*Figure A-8 GigabitEthernet QoS—Policy Map, Class Map, and Police Action Configuration Objects*


Note the following about the sample QoS configuration:

- Because the policy map pm-1Meg is attached to an input and an output interface:
  - Two cbQosObjectsIndex values are used (one for the input interface, the other for the output)
  - A single cbQosConfigIndex is used for both the input and the output objects
- Policy maps that are not attached to an interface are not included with SNMP data or displayed by the **show policy-map interface** command. This is why pm-1Meg is shown but pm1 is not.
- The default class map is always included with the SNMP data.
- Class maps that have no action defined are not included with the SNMP data. This is why cm1 is not part of cbQosCMCfgTable.

Figure A-9 shows an example of RED configuration information stored in MIB tables. Note that this configuration is applied to an ATM interface, not Gigabit Ethernet.

*Figure A-9 ATM QoS—RED Configuration Objects*




# Monitoring QoS

This section provides information about how to monitor QoS on the router by checking the QoS statistics in the MIB tables described in Table A-1. For information about how to determine the amount of traffic to bill customers for, see the "Billing Customers for Traffic" section on page A-44.

**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 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. |
| 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 figures, these counters are shown as 33-bit counters.

When accessing QoS statistics in counters, 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 *cbQosxxx* MIB objects.
  - Access the upper 32 bits of the counter through *cbQosxxxOverflow* MIB objects.

## QoS Statistics Tables

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

- Figure A-10 shows the counters in the cbQosCMStatsTable and the indexes for accessing these and other statistics.
- Figure A-11 shows the counters in cbQosMatchStmtStatsTable, cbQosPoliceStatsTable, cbQosQueueingStatsTable, cbQosTSStatsTable, and cbQosREDClassStatsTable.

See the "Sample QoS Statistics" section on page A-37 for examples of QoS statistics stored in tables.

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
```

**Note** Due to implementation features, some of the QoS statistics counters might wrap before they reach the maximum value they can accommodate.

***Figure A-10 QoS Class Map Statistics and Indexes***

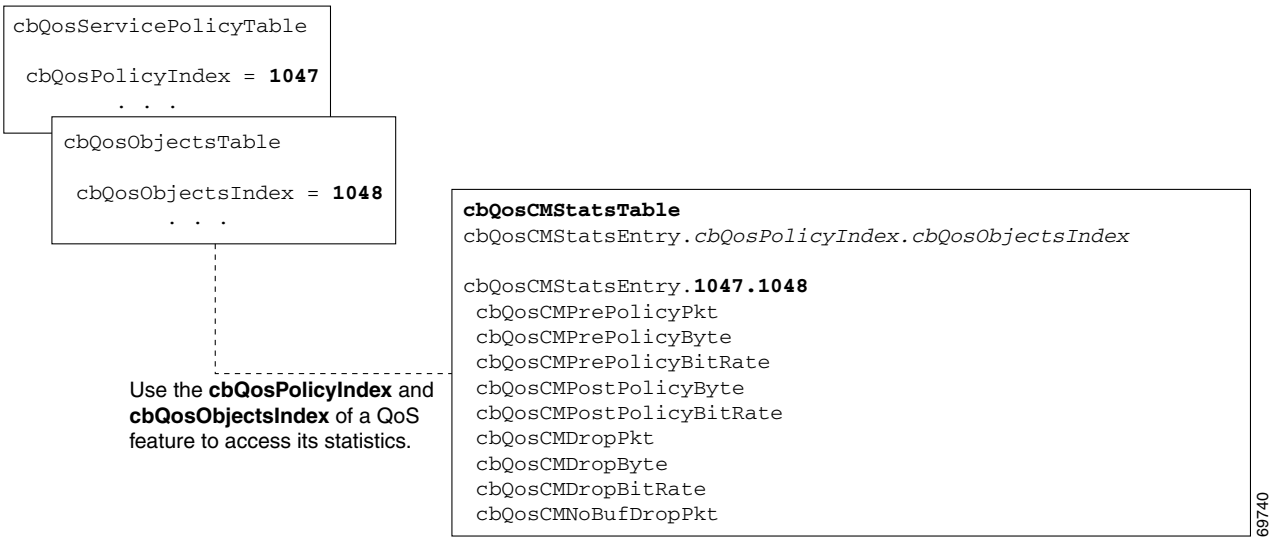
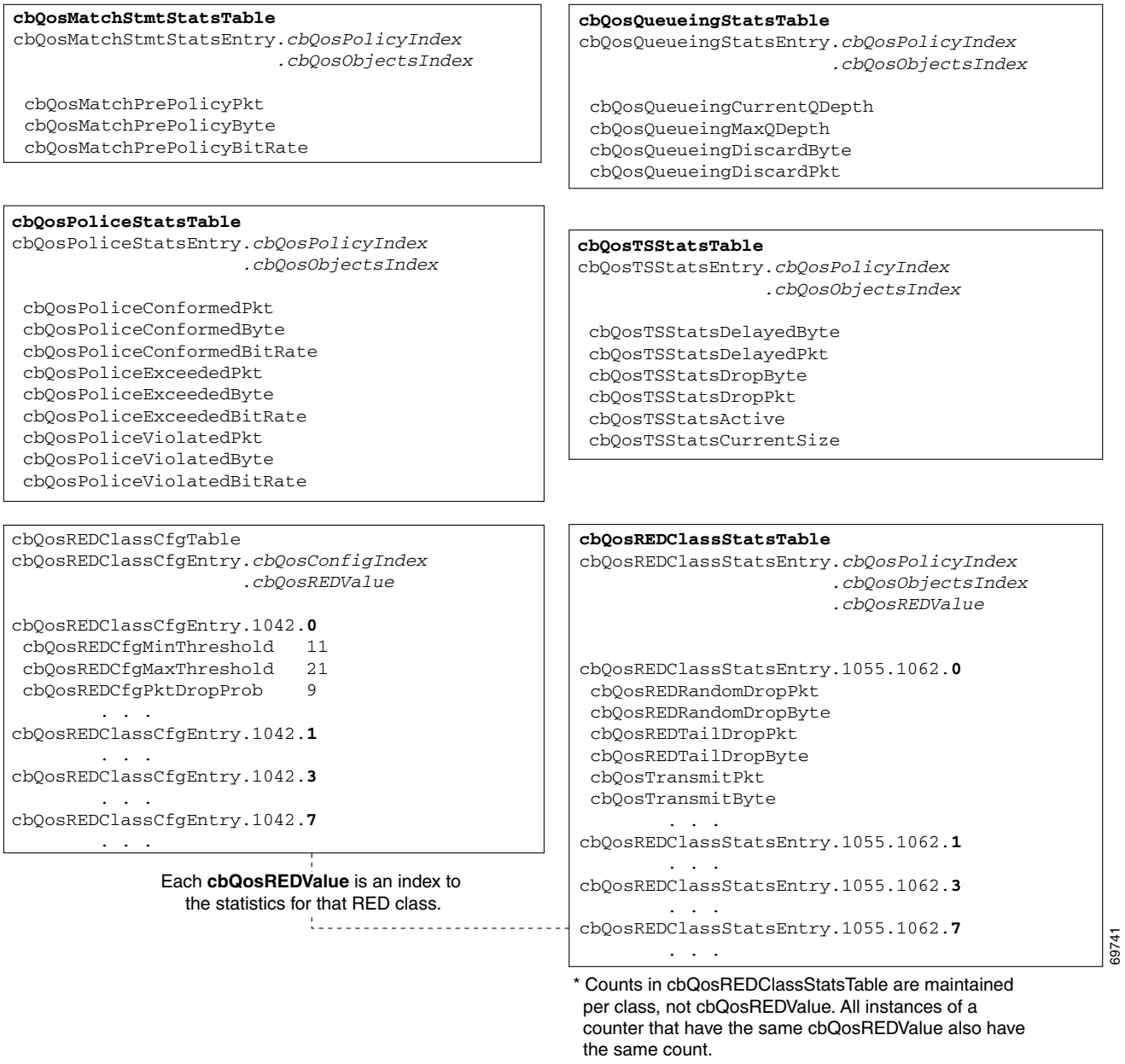


*Figure A-11 QoS Statistics Tables*




* 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 Statistics

This section contains figures that show how QoS statistics are displayed in show commands and stored in CISCO-CLASS-BASED-QOS-MIB tables.

- Figure A-12 shows an example of QoS statistics displayed by the **show policy-map interface** command.
- Figure A-13 on page A-39 shows class map statistics for the input service policy.
- Figure A-14 on page A-40 shows class map statistics for the output service policy.

- Figure A-15 on page A-41 shows match statement statistics for the input and output service policies.

***Figure A-12 Sample QoS Statistics—CLI show Commands***

```
c10k# show running-config interface GigabitEthernet 1/0/0.1
Building configuration...

Current configuration : 188 bytes
!
interface GigabitEthernet1/0/0.1
 encapsulation dot1Q 1
 ip address 10.1.0.2 255.255.255.0
 no ip directed-broadcast
 service-policy input pm-1meg
 service-policy output pm-1meg
end

c10k# show policy-map interface
 GigabitEthernet1/0/0.1

  Service-policy input: pm-1meg (2428)

    Class-map: class-default (match-any) (2429/0)
      4801508 packets, 667409423 bytes
      5 minute offered rate 1668000 bps, drop rate 667000 bps
      Match: any  (2431)
        4801508 packets, 667409423 bytes
        5 minute rate 1668000 bps
      Police:
        1000000 bps, 8000 limit, 8000 extended limit
        conformed 2878916 packets, 400169135 bytes; action: transmit
        exceeded 1922592 packets, 267240288 bytes; action: drop

  Service-policy output: pm-1meg (2433)

    Class-map: class-default (match-any) (2434/0)
      14259374 packets, 1925015267 bytes
      5 minute offered rate 1639000 bps, drop rate 640000 bps
      Match: any  (2436)
        14259374 packets, 1925015267 bytes
        5 minute rate 1639000 bps
      Output queue: 0/8192; 3698585/514006021 packets/bytes output, 0 drops
      Police:
        1000000 bps, 8000 limit, 8000 extended limit
        conformed 3517209 packets, 474822992 bytes; action: transmit
         exceeded 10742165 packets, 1450192275 bytes; action: drop c10k#
```

69742

*Figure A-13 QoS Class Map Statistics—Input Service Policy*

***Figure A-14 QoS Class Map Statistics—Output Service Policy***

```
c10k# show policy-map interface
 GigabitEthernet1/0/0.1
        . . .

Service-policy output: pm-1meg (2433)

   Class-map: class-default (match-any) (2434/0)
       14259374 packets, 1925015267 bytes
       5 minute offered rate 1639000 bps, drop rate 640000 bps
     Match: any  (2436)
       14259374 packets, 1925015267 bytes
       5 minute rate 1639000 bps
     Output queue: 0/8192; 3698585/514006021 packets/bytes output, 0 drops
     Police:
       1000000 bps, 8000 limit, 8000 extended limit
       conformed 3517209 packets, 474822992 bytes; action: transmit
       exceeded 10742165 packets, 1450192275 bytes; action: drop
```

```
cbQosCMCfgTable
 cbQosCMName = class-default
 cbQosCMInfo = matchAny(3)

cbQosObjectsTable
 cbQosObjectsIndex = 1909
 cbQosObjectsType = classmap(2)
 cbQosParentObjectsIndex = 1908

cbQosServicePolicyTable
 cbQosPolicyIndex = 1908
 cbQosIfType = subinterface(2)
 cbQosPolicyDirection = output(2)
```

**cbQosCMStatsTable**
cbQosCMStatsEntry.*cbQosPolicyIndex*.*cbQosObjectsIndex*

| cbQosCMStatsEntry.**1908.1909** | |
|---|---|
| cbQosCMPrePolicyPktOverflow | 0 |
| cbQosCMPrePolicyPkt | 14259374 |
| cbQosCMPrePolicyPkt64 | 0x000d994ae |
| cbQosCMPrePolicyByteOverflow | 0 |
| cbQosCMPrePolicyByte | 1925015267 |
| cbQosCMPrePolicyByte64 | 0x072bd66e3 |
| cbQosCMPrePolicyBitRate | 1639000 |
| cbQosCMPostPolicyByteOverflow | 0 |
| cbQosCMPostPolicyByte | 475598027 |
| cbQosCMPostPolicyByte64 | 0x01c590ccb |
| cbQosCMPostPolicyBitRate | 999000 |
| cbQosCMDropPktOverflow | 0 |
| cbQosCMDropPkt | 10742165 |
| cbQosCMDropPkt64 | 0x000a3e995 |
| cbQosCMDropByteOverflow | 0 |
| cbQosCMDropByte | 1449417240 |
| cbQosCMDropByte64 | 0x056645a18 |
| cbQosCMDropBitRate | 640000 |
| cbQosCMNoBufDropPktOverflow | 0 |
| cbQosCMNoBufDropPkt | 0 |
| cbQosCMNoBufDropPkt64 | 0x000000000 |

69744

*Figure A-15 QoS Match Statement Statistics*


# Sample QoS Applications

This section presents examples of sample 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 sample code shows how to:

- 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 whether 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 whether a service policy has been associated with the transmit and receive directions of a customer interface. Mark non-customer 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;
```

# Billing Customers for Traffic

This section describes how to use SNMP QoS information to determine the amount of traffic to bill to your customers. It also includes a scenario for demonstrating that a QoS service policy attached to an interface is policing traffic on that interface.

This section describes the following topics:



## 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. 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 will need this information in the following steps.

**Step 3** Access the cbQosPoliceConformedPkt object (cbQosPoliceStatsTable) for the customer to determine how much traffic on the interface is billable to this customer.

**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 has been 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 10000 series ESR 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 10000 Series Router Software Configuration Guide*.

```
policy-map police-out
  class BGPclass
    police 8000 1000 2000 conform-action transmit exceed-action drop

interface GigabitEthernet1/0/0.10
 description VLAN voor klant
 encapsulation dot1Q 10
 ip address 10.0.0.17 255.255.255.248
 service-policy output police-out
```

## 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

```
c10k# show policy-map interface g6/0/0.10

GigabitEthernet6/0/0.10

Service-policy output: police-out

   Class-map: BGPclass (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
```

```
      Match: access-group 101
      Police:
        8000 bps, 1000 limit, 2000 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop

   Class-map: class-default (match-any)
      4 packets, 292 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Output queue: 0/8192; 2/128 packets/bytes output, 0 drops
```

### SNMP Output

```
c10k# getone -v2c 10.86.0.63 public ifDescr.65
ifDescr.65 = GigabitEthernet6/0/0.10-802.1Q vLAN subif
```

## Generating Traffic

The following set of **ping** commands generates traffic:

```
c10k# ping
Protocol [ip]:
Target IP address: 10.0.0.18
Repeat count [5]: 99
Datagram size [100]: 1400
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.

Sending 100, 1400-byte ICMP Echos to 10.0.0.18, timeout is 1 seconds:
.!!.!..!.!..!.!..!.!..!.!..!.!.!..!.!..!.!..!.!..!.!..!.!..!.!.!..
!.!..!.!..!.!.!..!.!..!.!..!.!
Success rate is 42 percent (42/100), round-trip min/avg/max = 1/1/1 ms
```

## Packet Counts after the Service Policy Is Applied

After you generate traffic using the **ping** command, look at the number of packets that exceeded and conformed to the committed access rate (CAR) set by the **police** command:

- 42 packets conformed to the police rate and were transmitted
- 57 packets exceeded the police rate and were dropped

The following CLI and SNMP output show the counts on the interface after the service policy is applied. (In the output, conformed and exceeded packet counts are shown in boldface.)

### CLI Command Output

```
c10k# show policy-map interface g6/0/0.10

GigabitEthernet6/0/0.10

Service-policy output: police-out

   Class-map: BGPclass (match-all)
      198 packets, 281556 bytes
      30 second offered rate 31000 bps, drop rate 11000 bps
      Match: access-group 101
      Police:
        8000 bps, 1000 limit, 2000 extended limit
```

```
        conformed 42 packets, 59892 bytes; action: transmit
        exceeded 57 packets, 81282 bytes; action: drop

    Class-map: class-default (match-any)
       15 packets, 1086 bytes
       30 second offered rate 0 bps, drop rate 0 bps
       Match: any
       Output queue: 0/8192; 48/59940 packets/bytes output, 0 drops
```

### SNMP Output

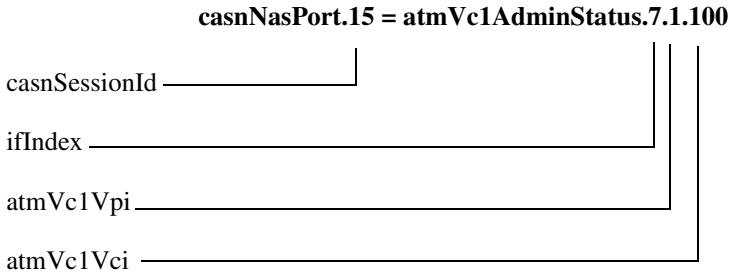
```
c10k# getmany -v2c 10.86.0.63 public ciscoCBQosMIB
        . . .
      cbQosCMDropPkt.1143.1145 = 57
        . . .
      cbQosPoliceConformedPkt.1143.1151 = 42
        . . .
```

# Using CISCO-AAA-SESSION-MIB

The following object support was added to the CISCO-AAA-SESSION-MIB to improve interface mapping sessions:

- casnNasPort—Identifies a particular conceptual row associated with the session identified by casnSessionId. The conceptual row that this object points to represents a port that is used to transport a session. If the port transporting the session cannot be determined, the value of this object will be zeroDotZero

  For example, a session is established using an ATM PVC. If the ifIndex of the ATM interface is 7 and the VPI/VCI values of the PVC are 1, 100 respectively, then the value of this object is (in this example):




  Where atmVc1AdminStatus is the first accessible object of the atmVcTable of the ATM-MIB.

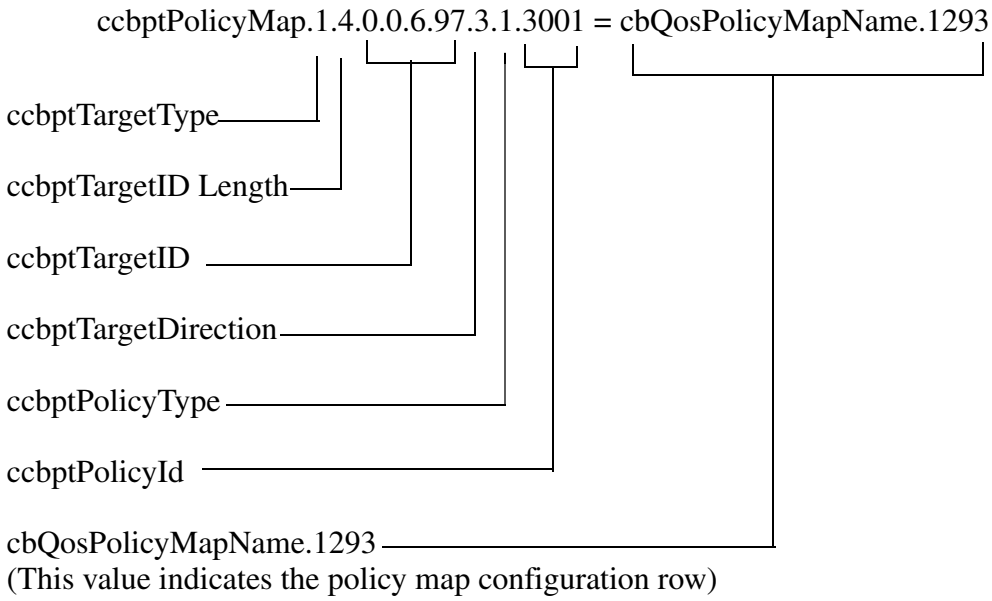
- casnVaiIfIndex—Identifies the ifIndex of the Virtual Access Interface (VAI) that is associated with the PPP session. This interface may not be represented in the IF-MIB in which case the value of this object will be zero.

# Using CISCO-CBP-TARGET-MIB

The CISCO-CBP-TARGET-MIB contains objects that define textual conventions for representing targets which have class based policy mappings. A target can be any logical interface or entity to which a class based policy is able to be applied.

The ccbptTarget is a series of octets that should be interpreted according to the value of ccbptTargetType.

The following is only one example of an index with the type genIf(1) and how to decode index values corresponding to config mapping data output.




The figure above indicates the mapping of the index portion of the object identifier (OID) for an instance of the ccbptPolicyMap object. Each portion of the index is defined below.

```
Config Policy Mapping Data
------------------------------
    ccbptPolicyMap.1.4.0.0.6.97.3.1.3001 = cbQosPolicyMapName.1293
```

Where from left to right:

- ccbptTargetType—Value of **1** indicates the ccbptTargetType which is genIf(1). The target type indicates that the value contained in the ccbptTargetId is an ifIndex value.
- ccbptTargetId Length—Value of **4** indicates that the length of the ccbptTargetId to follow is 4 bytes. The ccbptTargetId is defined in the MIB as a variable length OCTET-STRING representing it in the index of a table requires that it be preceded by the length of an octet string.
- ccbptTargetId—Value of 0.0.6.97 indicates the target ID. The length of the third index is determined by the value in the second byte of the entire index (in this example, the length of the target ID is 4 bytes). For supported ccbptTargetID values, see Possible Values for ccbptTargetID.

### Numerical Value for the ifIndex Example

The numerical value of this if Index ccbptTargetID, 0.0.6.97, is defined below.

(bits) 0—— 7 8—— 15 16—— 23 24—— 31

97 6 0 0

97 +

6* 2^8 (256) = 6*256 = 1536

1633 = numeric value of the ccbptTargetID, 0.0.6.97

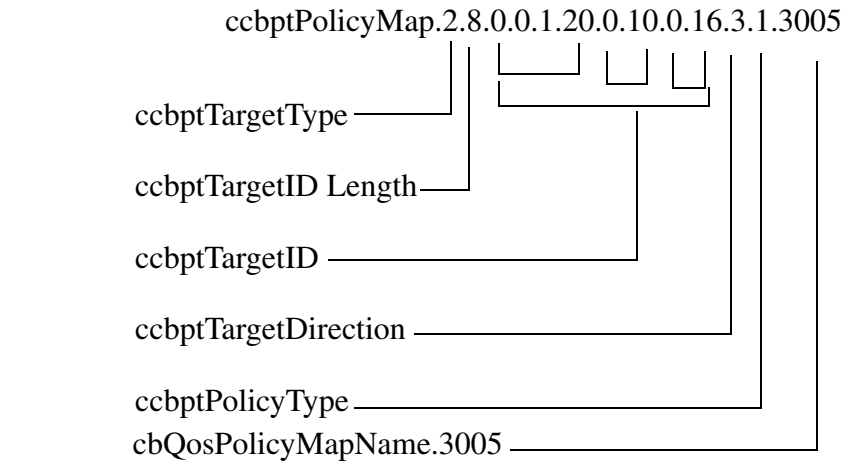
- ccbptTargetDirection—Value of **3** indicates the ccbptTarget output direction.
- ccbptPolicyType—Value of **1** indicates the ccbptPolicyType which is ciscoCbQos(1).
- ccbptPolicyId—Value of **3001** indicates the ccbptPolicyId which is the policy index integer for the policy instance applied to the target.

  Value is an unsigned32 (1.. 4294967295) which in this example the ccbptPolicyId equals the cbQosPolicyIndex which is the index to the CbQosService PolicyTable from the CISCO-CLASS-BASED-QOS-MIB.
- **cbQosPolicyMapName.1293** value indicates the row in the cbQosPolicyMapTable describing the configuration of the policy map applied to the output direction of this ccbptTargetId.

#### Possible Values for ccbptTargetID

The supported ccbptTargetID values are:

- For genIf(1), OCTECSTRING (SIZE(4)) – ifIndex (4d). Where the ( 4d) value is a four-byte decimal for the length of the ccbptTargetId in our example.
- For atmPvc(2), OCTET STRING (SIZE(8)) – ATM PVC (4d:2d:2d). Where the ATM PVC has a ccbptTargetId length of 8 bytes (4d:2d:2d). For example:




4d: = 0.0.1.20 = ifIndex
2d:= 0.10 = VPI
2d: = 0.16 = VCI

  - For frDlci(3), OCTET STRING(SIZE(6)) – Frame Relay ifIndex is first 4 bytes and DLCI is the last 2 bytes (4d:2d)
  - For controlPlane(4), OCTET STRING(SIZE(4)) – Control Plane Entity (4d)

# 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 3 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.inbiz

  Serial number format is defined in four fields:

  - Location (L)
  - Year (Y)
  - Workweek (W)
  - Sequential serial ID (S)

  The SN label will be 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.

# GLOSSARY

## A

**AAA** Authentication, authorization, and accounting.

**Alarm** The word alarm represents a condition that causes a trap to be generated.

**Alarm Severity** Each alarm type defined by a vendor type and employed by the system is assigned an associated severity. See critical, major, minor and informational for severity types.

**ATM** Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

**ATM-AAL5** ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented variable bit rate (VBR) services and is used predominantly for the transfer of classical IP over ATM and LAN emulation (LANE) traffic. AAL5 uses simple and efficient AAL (SEAL) and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

## 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.

**CNEM** Consistent Network Element Manageability.

**Collector** The NetFlow Collector receives Flow Records from one or more Exporters. It processes the received export packet, i.e. parses, stores the Flow Record information. The flow records may be optionally aggregated before storing into the hard disk.

**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.

## D

**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.

## E

**Egress Flows** Provides a mechanism to identify a flow as either an ingress or an egress flow."

**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 async 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.

**Exporter** A device (for example, a router) with NetFlow services enabled. The exporter monitors packets entering an observation point and creates flows out of these packets. The information from these flows are exported in the form of Flow Records to the collector.

## F

**Flow** An unidirectional sequence of packets between a given source and destination endpoints. Network flow endpoints are identified both by IP address as well as by transport layer application port numbers. NetFlow also utilizes the IP Protocol type, Type of Service (ToS), and the input interface identifier to uniquely identify flows.

**Flow record** Provides information about an IP Flow that exists on the Exporter. The Flow Records are commonly referred to as NetFlow Services data or NetFlow data.

**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.

**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.

## G

**Gb** gigabit

**Gbps** gigabits per second

**GB** gigabyte

**GBps** gigabytes per second

## 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.

**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.

**Interface Driver** A subsystem responsible for providing a layer of abstractionbetween device drivers or other data path components and the IOS operating environment.

**Interface Manager** A framework that facilitates a common control point betweenIOS applications and interface drivers.

**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

None

## 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.

**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.

## 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.

**NPE** Network Processing Engine.

**NSE** Network Service Engine.

## 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. The process responsible for monitoring the insertion and removal of modules during normal system operation.

## 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.

**PLIM** Physical layer interface module. Any module such as a field replaceable unit, that supports one or more physical network interfaces such as a line card, PA, or SPA.

**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/univercd/cc/td/doc/product/software/ios103/mib_doc/80516.htm#xtocid13

**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).

**SFP** Small formfactor pluggable transceiver.

**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.

## T

**TE** Traffic Engineered

**Template** NetFlow Version 9 Export format is template-based. Version 9 record format consists of a packet header followed by at least one or more template or data FlowSets. A template FlowSet (collection of one or more template) provides a description of the fields that will be present in future data FlowSets. Templates provide an extensible design to the record format to NetFlow services without requiring concurrent changes to the basic flow-record format.

One additional record type is also a part of Version 9 specification which is an options template rather than supplying information about IP flows, options are used to supply meta-data about the NetFlow process itself.

**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.

**Top Flows** Provides a mechanism which allows the top N flows in the netflow cache to be viewed in real time. Criteria can be set to limit the feature to particular flows of interest, which can aid in DoS detection. Only the number of flows (TopN) and the sort criteria (SortBy) need be set. Top Flows is not intended as a mechanism for exporting the entire netflow cache.

**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.

**UDP** User Datagram Protocol. A connections, non-reliable IP based transport 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.

## W

**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

## X

None

## Y

None

## Z

None

# INDEX

## A



## B



## C

## D



## E



## F



## I



## J



## L



## M

## N



## O



## P



## Q

## R



## S



## T



## U



## W