Cisco CMTS Universal Broadband Router MIB Specifications Guide

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-4952-08

Cisco CMTS Universal Broadband Router MIB Specifications Guide

CONTENTS

Preface xv

Document Revision History 3-xv

Audience 3-xix

Organization 3-xix

Obtaining Documentation and Submitting a Service Request xx

3-xx

CHAPTER 1 **Cisco CMTS Router MIB Overview** 1-1

MIB Description 1-1

Benefits of MIB Enhancements 1-2

MIB Dependencies 1-2

MIB Types 1-3

Object Identifiers 1-3

SNMP Overview 1-4

SNMP Notifications 1-5

SNMP Versions 1-5

Requests for Comments 1-7

Related Information and Useful Links 1-7

Cisco Technical Support Information and FAQs 1-8

SNMP Configuration Information 1-8

Cisco CMTS Documentation 1-8

Specifications and Standards 1-8

CHAPTER 2 **Configuring SNMP and MIB Support** 2-1

Determining MIB Support for Cisco IOS Releases 2-1

Cisco MIBs Supported By Product 2-1

Using the MIBs in Images Mail Service 2-2

Downloading and Compiling MIBs 2-3

Considerations for Working with MIBs 2-3

Downloading MIBs 2-4

Compiling MIBs 2-4

Enabling SNMP Support 2-4

High CPU Usage When Polling Routing ARP Tables 2-5

Enabling CEF Fast Switching on the Router 2-6
Using snmp-server view Commands 2-6
Using SNMP MIBs in DOCSIS 3.0 Downstream Solution 2-7
Using the Cisco MIB Locator 2-7
Additional References 2-8

CHAPTER 3 **MIB Specifications** 3-1
Overview of MIB Support 3-1
MIB Specifications 3-7
ATM-MIB 3-7
MIB Constraints 3-8
BGP4-MIB 3-8
MIB Constraints 3-8
BRIDGE-MIB 3-8
MIB Constraints 3-8
CISCO-AAA-SERVER-MIB 3-8
MIB Constraints 3-9
CISCO-AAL5-MIB 3-9
MIB Constraints 3-9
CISCO-ACCESS-ENVMON-MIB 3-9
MIB Constraints 3-9
CISCO-ATM-EXT-MIB 3-10
MIB Constraints 3-10
CISCO-ATM-PVCTRAP-EXTN-MIB 3-10
MIB Constraints 3-10
CISCO-BGP4-MIB 3-10
MIB Constraints 3-10
CISCO-BGP-POLICY-ACCOUNTING-MIB 3-11
MIB Constraints 3-11
CISCO-BULK-FILE-MIB 3-11
MIB Constraint 3-11
CISCO-BUS-MIB 3-11
MIB Constraints 3-11
CISCO-CABLE-ADMISSION-CTRL-MIB 3-12
MIB Constraints 3-12
CISCO-CABLE-AVAILABILITY-MIB 3-12
MIB Constraints 3-13

CISCO-CABLE-METERING-MIB 3-13
MIB Constraints 3-13
CISCO-CABLE-QOS-MONITOR-MIB 3-13
MIB Constraints 3-14
CISCO-CABLE-SPECTRUM-MIB 3-14
MIB Constraints 3-14
MIB Group Objects 3-15
CISCO-CABLE-WIDEBAND-MIB 3-16
MIB Notes and Constraints 3-17
CISCO-CALL-HISTORY-MIB 3-19
MIB Constraints 3-19
CISCO-CAR-MIB 3-19
MIB Constraints 3-19
CISCO-CASA-FA-MIB 3-20
MIB Constraints 3-20
CISCO-CASA-MIB 3-20
MIB Constraints 3-20
CISCO-CDP-MIB 3-20
MIB Constraints 3-20
CISCO-CIRCUIT-INTERFACE-MIB 3-21
MIB Constraints 3-21
CISCO-CLASS-BASED-QOS-MIB 3-21
MIB Constraints 3-21
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB 3-25
MIB Constraints 3-25
CISCO-CONFIG-COPY-MIB 3-25
MIB Constraints 3-25
CISCO-CONFIG-MAN-MIB 3-26
MIB Constraints 3-26
CISCO-DOCS-EXT-MIB 3-26
MIB Constraints 3-27
CISCO-DOCS-REMOTE-QUERY-MIB 3-29
MIB Constraints 3-30
CISCO-ENHANCED-MEMPOOL-MIB 3-30
MIB Constraints 3-31
CISCO-ENTITY-ALARM-MIB 3-31
MIB Constraints 3-31
CISCO-ENTITY-ASSET-MIB 3-31

MIB Constraint 3-32
CISCO-ENTITY-EXT-MIB 3-32
MIB Constraints 3-32
CISCO-ENTITY-FRU-CONTROL-MIB 3-32
MIB Constraints 3-32
CISCO-ENTITY-SENSOR-MIB 3-33
MIB Constraints 3-33
CISCO-ENTITY-VENDORTYPE-OID-MIB 3-34
MIB Constraints 3-34
CISCO-ENVMON-MIB 3-37
MIB Constraints 3-37
CISCO-FLASH-MIB 3-39
MIB Constraints 3-39
CISCO-FRAME-RELAY-MIB 3-39
MIB Constraints 3-40
CISCO-FTP-CLIENT-MIB 3-40
MIB Constraints 3-40
CISCO-HSRP-EXT-MIB 3-40
MIB Constraints 3-40
CISCO-HSRP-MIB 3-40
MIB Constraint 3-41
CISCO-IETF-ATM2-PVCTRAP-MIB 3-41
MIB Constraint 3-41
CISCO-IETF-IP-FORWARD-MIB 3-41
MIB Constraints 3-41
CISCO-IETF-IP-MIB 3-41
MIB Constraints 3-42
CISCO-IETF-NAT-MIB 3-42
MIB Constraints 3-42
CISCO-IMAGE-MIB 3-42
MIB Constraints 3-42
CISCO-IP-ENCRYPTION-MIB 3-43
MIB Constraints 3-43
CISCO-IPMROUTE-MIB 3-43
MIB Constraints 3-43
CISCO-IP-STAT-MIB 3-43
MIB Constraints 3-43

CISCO-IPSEC-FLOW-MONITOR-MIB 3-44
MIB Constraints 3-44
CISCO-IPSEC-MIB 3-44
MIB Constraint 3-44
CISCO-IPSEC-POLICY-MAP-MIB 3-44
MIB Constraint 3-44
CISCO-ISDN-MIB 3-44
MIB Constraint 3-45
CISCO-LEC-DATA-VCC-MIB 3-45
MIB Constraints 3-45
CISCO-LEC-EXT-MIB 3-45
MIB Constraints 3-45
CISCO-LECS-MIB 3-45
MIB Constraints 3-46
CISCO-LES-MIB 3-46
MIB Constraints 3-46
CISCO-MEMORY-POOL-MIB 3-46
MIB Constraints 3-46
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB 3-46
MIB Constraints 3-47
CISCO-NDE-MIB 3-47
MIB Constraints 3-47
CISCO-NTP-MIB 3-47
MIB Constraints 3-47
CISCO-PIM-MIB 3-48
MIB Constraints 3-48
CISCO-PING-MIB 3-48
MIB Constraints 3-48
CISCO-PPPOE-MIB 3-48
MIB Constraints 3-48
CISCO-PROCESS-MIB 3-48
MIB Constraints 3-49
CISCO-PRODUCTS-MIB 3-49
MIB Constraints 3-49
CISCO-QUEUE-MIB 3-50
MIB Constraints 3-50
CISCO-RMON-SAMPLING-MIB 3-50
MIB Constraints 3-50

CISCO-RTTMON-MIB 3-50
CISCO-SLB-EXT-MIB 3-51
MIB Constraints 3-51
CISCO-SLB-MIB 3-51
MIB Constraints 3-51
CISCO-SNAPSHOT-MIB 3-51
MIB Constraints 3-52
CISCO-SRP-MIB 3-52
MIB Constraints 3-52
CISCO-SYSLOG-MIB 3-52
MIB Constraints 3-52
CISCO-TCP-MIB 3-52
MIB Constraint 3-53
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB 3-53
MIB Constraint 3-53
CISCO-VPDN-MGMT-EXT-MIB 3-53
MIB Constraints 3-53
CISCO-VPDN-MGMT-MIB 3-54
MIB Constraints 3-54
CISCO-VSIMASTER-MIB 3-55
MIB Constraints 3-55
DOCS-BPI-MIB 3-55
MIB Constraints 3-55
DOCS-BPI-PLUS-MIB 3-55
MIB Constraints 3-56
DOCS-CABLE-DEVICE-MIB 3-56
MIB Constraints 3-57
DOCS-CABLE-DEVICE-TRAP-MIB 3-57
MIB Constraints 3-58
DOCS-IF-EXT-MIB 3-58
MIB Constraints 3-58
DOCS-IF-MIB 3-58
MIB Constraints 3-59
DOCS-DSG-IF-MIB 3-62
MIB Constraints 3-63
DOCS-QOS-MIB 3-64
MIB Constraints and Notes 3-64

DOCS-SUBMGT-MIB 3-66
MIB Constraints 3-66
DTI-MIB 3-67
MIB Constraints 3-68
ENTITY-MIB 3-68
MIB Constraints 3-69
Cisco uBR100012 SPA-24XWBD-SFP Shared Port Adapter 3-72
ENTITY-MIB UDI Support 3-72
Overview of the ENTITY-MIB 3-73
Changes to Support Virtual Interfaces 3-76
Chassis Slot Layout 3-77
ETHERLIKE-MIB 3-77
MIB Constraints 3-77
EVENT-MIB 3-78
MIB Constraints 3-78
EXPRESSION-MIB 3-78
MIB Constraints 3-78
HC-RMON-MIB 3-79
MIB Constraints 3-79
IF-MIB 3-79
IF-MIB Notes 3-79
IF-MIB Notes for Cisco IOS Release 12.3(23)BC 3-81
IGMP-MIB 3-83
MIB Constraints 3-83
IGMP-STD-MIB 3-83
MIB Constraint 3-83
INT-SERV-MIB 3-83
MIB Constraints 3-84
IP-MIB 3-84
MIB Constraint 3-84
IPMROUTE-MIB 3-84
MIB Constraint 3-84
IPMROUTE-STD-MIB 3-84
MIB Constraint 3-85
ISDN-MIB 3-85
MIB Constraint 3-85
LAN-EMULATION-CLIENT-MIB 3-85
MIB Constraints 3-85

MSDP-MIB 3-85
MIB Constraints 3-86
NOTIFICATION-LOG-MIB 3-86
MIB Constraints 3-86
nruCacheSnmpData 3-86
MIB Constraints 3-87
OLD-CISCO-CHASSIS-MIB 3-87
OLD-CISCO-CPU-MIB 3-87
OLD-CISCO-INTERFACES-MIB 3-87
OLD-CISCO-IP-MIB 3-88
OLD-CISCO-MEMORY-MIB 3-88
OLD-CISCO-SYSTEM-MIB 3-88
OLD-CISCO-TCP-MIB 3-88
OLD-CISCO-TS-MIB 3-88
PIM-MIB 3-88
MIB Constraints 3-89
RFC1213-MIB 3-89
MIB Constraints 3-89
RFC1231-MIB 3-89
MIB Constraint 3-89
RFC1253-MIB 3-89
MIB Constraints 3-90
RFC1315-MIB 3-90
MIB Constraints 3-90
RFC1381-MIB 3-90
MIB Constraint 3-90
RFC1382-MIB 3-90
MIB Constraint 3-91
RFC1406-MIB 3-91
MIB Constraints 3-91
RFC1407-MIB 3-91
MIB Constraints 3-91
RFC1595-MIB 3-91
MIB Constraint 3-92
RFC2558-MIB 3-92
MIB Constraints 3-92
RMON-MIB 3-92

MIB Constraints 3-92
RMON2-MIB 3-92
MIB Constraints 3-92
RS-232-MIB 3-93
MIB Constraints 3-93
RSVP-MIB 3-93
MIB Constraints 3-93
SMON-MIB 3-93
MIB Constraints 3-93
SNMP-COMMUNITY-MIB 3-93
MIB Constraints 3-94
SNMP-FRAMEWORK-MIB 3-94
MIB Constraints 3-94
SNMP-MPD-MIB 3-94
MIB Constraints 3-94
SNMP-NOTIFICATION-MIB 3-94
MIB Constraints 3-95
SNMP-PROXY-MIB 3-95
MIB Constraints 3-95
SNMP-TARGET-MIB 3-95
MIB Constraints 3-95
SNMP-USM-MIB 3-95
MIB Constraints 3-95
SNMP-VACM-MIB 3-96
MIB Constraints 3-96
SNMPv2-MIB 3-96
MIB Constraints 3-96
TCP-MIB 3-96
MIB Constraints 3-96
UDP-MIB 3-96
MIB Constraints 3-97

CHAPTER 4 **Monitoring Notifications** 4-1
SNMP Notification Overview 4-2
Enabling Notifications 4-2
Cisco SNMP Notifications 4-3
Functional Notifications 4-3

Cisco Router Line Card Notifications 4-5
Flash Card Notifications 4-7
Link Notifications 4-8
Packet Forwarding Engine Notifications 4-9
Configuration Notifications 4-10
MPLS Service Notifications 4-11
Interface Trap Descriptions 4-11
Routing Protocol Notifications 4-13
Interface Trap Descriptions 4-13
Routing Service Notifications 4-15
SONET Notifications 4-16
Chassis Notifications 4-17
RTT Monitor Notifications 4-18
Environmental Notifications 4-19
Redundancy Framework Notifications 4-20
Cable MIB Notifications 4-21

APPENDIX A **Using Cisco CMTS MIBs** A-1
Tips and Guidelines A-1
IF-MIB Caching A-1
SNMP-Based and CLI-Based Counters A-2
Redundant PRE Modules on the Cisco uBR10012 Router A-2
Obtaining Basic Information About the Router A-3
OLD-CISCO-CHASSIS-MIB A-3
SNMPv2-MIB A-3
ENTITY-MIB A-4
Managing Physical Components A-4
ENTITY-MIB A-5
Cisco-Specific MIBS A-6
Performing Inventory Management A-6
Generating SNMP Traps A-12
Monitoring SYSLOG Messages A-15
Message Table Objects A-15
Control Objects A-15
SYSLOG Notifications A-16
Example A-16
Displaying Information About Cable Modems A-17
Displaying Current Status for Cable Modems A-17
Displaying Information About Burst and Station Maintenance Intervals A-18

Logging and Displaying Deleted Service Flows A-19
Monitoring Spectrum Management A-20
Enabling Spectrum Management A-21
Displaying the Results of a Spectrum Request A-23
Monitoring CNR Measurements for Individual Cable Modems A-24
Displaying Information About Frequency Hops A-26
Using Flap Lists A-29
Configuring Flap List Operation Using SNMP A-29
Displaying the Flap List Using SNMP A-30
Displaying Flap-List Information for Specific Cable Modems A-32
Clearing the Flap List and Counters Using SNMP A-33
Using Subscriber Traffic Management A-34
Configuring and Displaying the Enforce Rules for Quality of Service A-34
Displaying Subscribers Who Have Violated Their Enforce Rules A-35
Notifications for Subscribers Who Have Violated Their Enforce Rules A-36
Usage-Based Billing A-36
Modes of Operation A-37
File Mode A-37
Usage-Based Billing Feature (File Mode) A-37
Streaming Mode A-38
Identifying Cisco Unique Device Identifiers A-41
DOCS-DSG-IF-MIB Validation Requirements A-41

APPENDIX B **Relationship Between MIB Objects and CLI Show Commands** B-1
CISCO-CABLE-QOS-MONITOR-MIB B-2
CISCO-DOCS-EXT-MIB B-3
CISCO-DOCS-REMOTE-QUERY B-10
DOCS-IF-MIB B-10
DOCS-QOS-MIB B-15
DOCS-SUBSCRIBER-MIB B-24

APPENDIX C **CMTS MIBs Supported in Cisco IOS Release 12.1(20)EC and IOS Release 12.3(9a)BC** C-1

GLOSSARY

INDEX

Preface

Revised: December 2007, OL-4952-08

This guide describes the implementation of the Simple Network Management Protocol (SNMP) for Cisco Cable Modem Termination System (CMTS) routers.

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 and network status or events.

This Preface provides an overview of this guide with the following sections:

- Document Revision History, page xv
- Audience, page xix
- Organization, page xix
- Obtaining Documentation and Submitting a Service Request, page xx

Document Revision History

The following 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.

Cisco IOS Release	Part Number	Publication Date
12.3(23)BC	OL-4952-08	December 2007

Description of Changes

Cisco IOS Release 12.3(23)BC introduces support for DOCSIS 3.0 Downstream Solution on the Cisco uBR10012 router and Cisco SIP and SPA. The following MIBs are introduced or enhanced further in Cisco IOS Release 12.3(23)BC for DOCSIS 3.0 Downstream Solution on the Cisco CMTS:

- CISCO-CABLE-SPECTRUM-MIB
- CISCO-CABLE-WIDEBAND-MIB
- CISCO-DOCS-EXT-MIB
- DOCS-DSG-IF-MIB
- DOCS-IF-MIB

- DTI-MIB
- DOCS-BPI-PLUS-MIB
- DOCS-CABLE-DEVICE-MIB
- DOCS-CABLE-DEVICE-TRAP-MIB
- ENTITY-MIB
- IF-MIB

Cisco IOS Release	Cisco RF Switch Firmware Version	Part Number	Publication Date
12.3(21)BC	3.80	OL-4952-06	August 2007

Description of Changes

Cisco RF Switch Firmware Version 3.80, installed on the Cisco RF Switch, supports the following changes or enhancements for SNMP MIBs on the Cisco RF Switch, to be used with Cisco IOS release 12.3BC on the Cisco CMTS:

- SNMP MIB get and set variables can be saved to cache in the AdminState MIB module. The SNMP Cache can be disabled or reenabled using the system-level **set snmp cache** firmware command. The setting for this command is stored in non-volatile memory on the Cisco RF Switch.
- Cisco RF Switch Firmware Version 3.80 adds a new MIB object identifier (OID) to control caching on the Cisco CMTS. To control caching in this manner, use the SNMP object nruCacheSnmpData, which is a read/write integer at OID 1.3.6.1.4.1.6804.2.1.1.9.
- Three system-level Cisco RF Switch firmware commands have been introduced or enhanced to reflect these additional caching functions and options:
  - **set snmp cache**
  - **show config**
  - **show module**

Refer to the following document on Cisco.com for additional command information:

- *Release Notes for Cisco RF Switch Firmware, Version 3.80*

  http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/release/notes/rfswrn36.html

Cisco IOS Release	Part Number	Publication Date
12.3(21)BC	OL-4952-05	February 2007

Description of Changes

- CISCO-CABLE-WIDEBAND-MIB support on the Cisco uBR10012 universal broadband router. Cisco Wideband Protocol supports downstream wideband channels consisting of multiple bonded RF channels.

Note CISCO-CABLE-WIDEBAND-MIB support is only on the uBR100012 CMTS router and is a Cisco proprietary MIB that supports the DOCSIS 3.0 standard.

  - Updated the ENTITY-MIB with the new wideband shared port adapter card, SPA-24XWBD-SFP support, OID 1.3.6.1.4.1.9.12.3.1.9.2.145. See Cisco uBR100012 SPA-24XWBD-SFP Shared Port Adapter, page 72 for the shared port adapter physical entities and values in the ENTITY-MIB.
  - Update the IF-MIB for interface wideband management support.
  - Added ccwbFiberNodeTable which provides configuration and topology information for Fiber nodes. See CISCO-CABLE-WIDEBAND-MIB, page 16.
  - Updated Cisco SNMP Notifications, page 3 with wideband cable trap support.
- Enhanced the CISCO-DOCS-EXT-MIB, page 26 with new table objects that can query both CM and CPE information.
- Added tables (docsQosParamSetEntry, docsQosServiceFlowEntry, docsQosServiceFlowStatsEntry, docsQosPHSEntry, docsQosPktClassEntry, docsQosUpstreamStatsEntry) to support SNMP enhancements in the DOCS-QOS-MIB. This enhancement significantly improves QoS MIB query time in a large scale system with much less CPU consumption.
- Enhanced CISCO-CABLE-SPECTRUM-MIB, page 14 with new tables and objects to support the retrieval of spectrum group information using SNMP query.
- Updated Cisco CMTS platform support for unique device identifier (UDI) compliance. Added support for the unique device identifier (UDI) standard which displays information from any Cisco product that has electronically stored identity information. See Overview of the ENTITY-MIB, page 73.
- Updated the CISCO-CABLE-METERING-MIB with the ccmtrCollectionSrcIfIndex object which is used to specify the source interface for billing packets.
- Added the docsIfCmtsChannelUtilizationInterval object to the DOCS-IF-MIB. This object provides operators with a mechanism to evaluate the load/utilization of both upstream and downstream physical channels. This information may be used for capacity planning and incident analysis, and may be particularly helpful in provisioning of high value QOS.
- Added support on the uBR10012and uBR7246VXR router platforms for the CISCO-CABLE-ADMISSION-CTRL-MIB

Note For detailed information about admission control for Cisco CMTS, go to the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.html

Cisco IOS Release	Part Number	Publication Date
12.3(17a)BC2	OL-4952-04	July 2006

Description of Changes

- Added the DOCS-DSG-IF-MIB, page 62.
- Added cable traps, Cable MIB Notifications, page 21.
- Added section describing the DOSCS-DSG-IF-MIB validation capabilities. See, DOCS-DSG-IF-MIB Validation Requirements, page 41.
- The CISCO-ENHANCED-MEMPOOL-MIB is supported on cable line cards.
- Added cable device traps. SeeCable MIB Notifications, page 21.

- DOCS-IF-MIB, page 58 is updated to draft-ietf-ipcdn-docs-rfmibv2-05.txt.
- IF-MIB, page 79 supports subinterfaces in the ifTable.
- Updated the CISCO-DOCS-EXT-MIB, page 26 for the Dynamic Shared Secret feature.

Cisco IOS Release	Part Number	Publication Date
12.3(17a)BC	OL-4952-03	February 2006

Description of Changes

- Added table (Table 3-2 on page 6) of cable-specific MIBs.
- Added Appendix C, CMTS MIBs Supported in Cisco IOS Release 12.1(20)EC and IOS Release 12.3(9a)BC—Tables list MIBs supported for past releases for the following universal broadband routers:
  - Cisco uBR7100 series and Cisco uBR7200 series for Cisco IOS Release 12.1(20)EC
  - Cisco uBR7100 series and Cisco uBR7200 series for Cisco IOS Release 12.3(9a)BC
  - Cisco uBR10012 for Cisco IOS Release 12.3(9a)BC
  - CISCO-AAA-SERVER-MIB
  - CISCO-ENTITY-ALARM-MIB
  - CISCO-ENTITY-EXT-MIB
  - CISCO-ENTITY-FRU-CONTROL-MIB
- Updated the following MIBs:
  - CISCO-CLASS-BASED-QOS-MIB—This MIB is now supported on the Cisco uBR10012 router
  - CISCO-DOCS-EXT-MIB—Supports the dynamic shared secret (DMIC) feature which ensures that every online cable modem uses the DOCSIS configuration file assigned to it. This protects against theft-of-service attempts from subscribers and safeguards operators against stolen or fraudulently downloaded configuration files.
  - ENTITY-MIB
  - CISCO-ENTITY-VENDORTYPE-OID-MIB—Updated OIDs.
  - CISCO-ENVMON-MIB
  - CISCO-CABLE-SPECTRUM-MIB notifications. See Cable MIB Notifications, page 21.
  - DOCS-QOS-MIB—MIB object information is updated to support DCC for load balancing.
- Updated Chapter 4, “Monitoring Notifications”—Added the following information:
  - 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
- Added the usage-based billing support feature to section, Usage-Based Billing, page 36. This feature was introduced on Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers.

Feature support includes the new CISCO-CABLE-METERING-MIB, which contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format

For complete documentation about using the Usage-Based Billing feature for Cisco CMTS, go to:

http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html

Cisco IOS Release	Part Number	Publication Date
12.3(9a)BC 12.1(20)EC	OL-4952-02	September 2004 (no revision table available). See Appendix C, "CMTS MIBs Supported in Cisco IOS Release 12.1(20)EC and IOS Release 12.3(9a)BC" for a list of the MIBs included in Cisco IOS Release 12.1(20)EC and Cisco IOS Release 12.3(9a)BC for Cisco CMTS routers.

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 CMTS Router MIB Overview," provides background information about SNMP and its implementation on Cisco CMTS routers.
- Chapter 2, "Configuring SNMP and 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 Cisco CMTS MIBs," describes how to perform common tasks on the router.
- Appendix B, "Relationship Between MIB Objects and CLI Show Commands," provides a cross-reference between commonly used objects in the MIBs and the related cable-related **show** commands.
- Appendix C, "CMTS MIBs Supported in Cisco IOS Release 12.1(20)EC and IOS Release 12.3(9a)BC" provides a list of Cisco CMTS MIBs from previous IOS releases.
- Glossary—Glossary provides a list of terms and the definitions.

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Cisco CMTS Router MIB Overview

This chapter provides an overview of the Cisco Cable Modem Termination System (CMTS) router. This chapter contains the following topics:

- MIB Description, page 1-1
- Benefits of MIB Enhancements, page 1-2
- MIB Dependencies, page 1-2
- MIB Types, page 1-3
- Object Identifiers, page 1-3
- SNMP Overview, page 1-4
- Related Information and Useful Links, page 1-7

MIB Description

A Management Information Base (MIB) is a collection of information that can be managed by the SNMP manager. The objects in a MIB are organized and identified by object identifiers (OID) that are defined by the IETF and other organizations. Cisco's implementation of SNMP uses MIBs that conform to the MIB II definition that is described in RFC 1213.

Objects can refer to a physical device (such as a line card or clock card or shared port adapter), a software parameter (such as an IP address or operation mode), or a run-time statistic (such as number of packets passed or temperature). When the device contains multiple objects of the same type, it appends a unique instance number to the end of the OID, so that the SNMP manager and agent can distinguish between the different objects.

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 interfaces on the router). Each row in a MIB table describes all of the parameters for a particular object (such as IP address, clock speed, number of ports, and so forth). SNMP managers can read or set all of the information in a row with one request.

  Typically, each row in a table is identified by a unique index number. Depending on the table, this index either could reflect a physical attribute (such as the slot number in a chassis or port number on a card) or it could be an arbitrary number (such as is used for tables that list error messages or packet statistics).

Each row also has a status object that shows whether the row is created, activated, deactivated, or deleted. When an SNMP manager creates a new row, it typically sets the row's status to create and then populates the row with the desired parameters. The SNMP agent does not use the objects in a row until the SNMP manager sets the row's status to activate. This ensures that the SNMP agent does not try to use a row's parameters until the SNMP manager has finished creating the row and entered all of the row's required parameters.

Benefits of MIB Enhancements

The Cisco CMTS uBR router enhanced management feature allows the router to be managed through the Simple Network Management Protocol (SNMP). The feature also expands the number of Management Information Bases (MIBs) included with the router.

Using the Cisco CMTS uBR router enhanced management feature, you can:

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

Other benefits include:

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

MIB Dependencies

The SNMP specifications define MIBs in a highly structured hierarchical format, in which MIBs that are lower in the hierarchy use objects that are defined by MIBs higher up in the hierarchy. Each MIB includes a section titled "IMPORTS" that lists the objects it uses that are defined by other MIBs.

For example, the IF-MIB, which defines standard objects for router interfaces, uses the following IMPORT block:

```
IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, Counter32, Gauge32, Counter64,
    Integer32, TimeTicks, mib-2,
    NOTIFICATION-TYPE                        FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, DisplayString,
    PhysAddress, TruthValue, RowStatus,
    TimeStamp, AutonomousType, TestAndIncr   FROM SNMPv2-TC
    MODULE-COMPLIANCE, OBJECT-GROUP,
    NOTIFICATION-GROUP                       FROM SNMPv2-CONF
    snmpTraps                                FROM SNMPv2-MIB
    IANAifType                               FROM IANAifType-MIB;
```

This section shows that the IF-MIB uses objects that are defined by the SNMPv2-SMI, SNMPv2-TC, SNMPv2-CONF, SNMPv2-MIB, and IANAifType-MIB MIBs. To use the IF-MIB with your SNMP management software, you must load these other MIBs as well.

Typically, most SNMP managers use the IMPORT blocks in the MIBs to automatically determine the order in which the MIBs must be loaded. However, if you are manually loading MIBs, you must do so in the proper order.

To determine the dependencies among MIBs, you can use the "View and Download MIBs" tool, which is part of the SNMP Object Navigator on the Cisco IOS MIB Tools page. This URL takes you to the MIB Locator:

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

MIB Types

MIBs on the Cisco CMTS can be arranged in the following categories:

- SNMP standard MIBs—Part of the SNMPv1, SNMPv2c, and SNMPv3 specifications and must be supported by any agent supporting SNMP network management. These MIBs provide the framework for SNMP management, defining common objects and interfaces.
- Internet standard MIBs—Provide generic definitions for objects that provide information about commonly used protocols, such as IP, TCP, and Internet Control Message Protocol (ICMP). These MIBs are typically defined by the IETF as Internet-Drafts and Request for Comments (RFCs).
- Cisco platform and network-layer enterprise MIBs—Provide information that is specific to Cisco platforms. These MIBs can extend standard MIBs by providing additional related information, or they can provide information about features that are specific to Cisco platforms. Typically, the same Cisco-specific MIB is used on all Cisco platforms that implement the MIB's particular feature. These MIBs are also typically updated whenever the related feature is updated in the Cisco IOS software.
- Cable-specific MIBs—Provide information about the cable interfaces and related information on the Cisco CMTS platforms. These MIBs can be divided into the following subcategories:
  - DOCSIS-specified MIBs—Defined by CableLabs, which created and maintains the DOCSIS specification. When the DOCSIS specifications have been finalized, these MIBs are also submitted to the IETF and are eventually released as RFCs. These MIBs can also include other services, such as DOCSIS Set-Top Gateway (DSG), as CableLabs continues to develop specifications for these additional cable services.
  - Cisco-specific cable MIBs—Provide extensions to the DOCSIS MIBs for features that are specific to Cisco platforms.
- Deprecated MIBs—Supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network management applications and scripts should convert to the replacement MIBs as soon as possible, because deprecated MIBs could be removed without notice.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed router or other network device. All OIDs are arranged in a hierarchical order, with top-level OIDs assigned by standards organizations such as IETF, ISO, and ITU. Lower-level OIDs are assigned by individual vendor organizations, such as Cisco Systems.

Each level in an OID is assigned both a number and a name. The hierarchical structure of the OIDs allow for easy translation between the number and name forms of an OID.

For example, SNMP standard MIBs that are intended for use by all vendors typically start with "1.3.6.1.2.1", which translates as follows:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)

Typically, vendor-specific MIBs have OIDs that start with "1.3.6.1.4.1", which translates as follows:

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1)

Cisco Systems was assigned the next OID of "9", so most OIDs for items that are specific to Cisco platforms start with "1.3.6.1.4.1.9":

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9)

For illustrative purposes, the OIDs above are shown with both number and name forms combined. Typically, only the name or number for a level is used. However, names and numbers can be mixed in the same OID. For example, the top-most Cisco-specific OID could also be given as either "1.3.6.1.4.1.cisco" or "iso.org.dod.internet.private.enterprises.9".

To translate OIDs between their name and number format, and to display the location of any OID in the OID tree, you can use the SNMP Object Navigator on the Cisco IOS MIB Tools page. This URL takes you to the MIB Locator:

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

For a listing of all of the objects and OIDs that are included in any particular MIB, you can download the text files at the following URL:

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

SNMP Overview

The Cisco CMTS routers can be managed through SNMP, which is an application-layer protocol that provides a standardized framework and a common language for monitoring and managing devices in a network. The SNMP framework has the following main parts:

- An SNMP manager—A system used to control and monitor the activities of network hosts by using SNMP commands. The most common managing system is called a network management system (NMS), which can be either a standalone device that is dedicated to network management, or a workstation that is running network management applications. Many network management applications are available and range from simple, freely available command-line applications to feature-rich, commercial products with sophisticated graphical user interfaces.
- An SNMP agent—A software component in a managed device that maintains the SNMP data and communicates with the SNMP manager. Typically, the agent is configured to respond only to one or more specific SNMP managers, so that unauthorized parties do not have access to the device. On the Cisco CMTS, the Cisco IOS software runs the SNMP agent software, but it does not become active until it is enabled using the command-line interface (CLI).
- Management Information Base (MIB)—Objects that can be managed by SNMP are defined in MIBs, which are ASCII text files in a structured format. MIBs that are standardized for use industry-wide among multiple vendors are created and maintained by organizations such as the Internet Engineering Task Force (IETF) and CableLabs. Vendors, such as Cisco, also create vendor-specific MIBs to manage vendor-specific platforms and features. On the Cisco CMTS, MIBs are part of the Cisco IOS software image. Typically, each new Cisco IOS software release includes MIBs that are new or have been modified.

The SNMP manager communicates with the SNMP agent in the following ways:

- GET requests—The SNMP manager obtains information from the device by sending GET requests to the agent. The manager can obtain this information one object at a time using single GET requests.
- SET requests—The SNMP manager configures the device by sending SET requests to the agent. The manager can configure one item at a time using single SET requests, or it can configure multiple parameters using a BULK-SET request.
- Notifications—The SNMP agent asynchronously informs the manager that specific events have occurred by using a trap or inform message (depending on the version of SNMP being used). The network administrator configures the agent for the types of traps and informs it should send. These can range from purely informational messages, such as traffic statistics, to important messages that warn of critical situations and errors, such as a card failure.

SNMP Notifications

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

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

When an agent detects an alarm condition, the agent:

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

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.

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

When an agent detects an alarm condition, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host. SNMP notifications can be sent as either *traps* or *informs*. See the for instructions on how to enable traps on the Cisco CMTS uBR router. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs. See Chapter 4, “Monitoring Notifications,” for information about Cisco CMTS uBR router notifications.

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 SNMPv2c (SNMPv2 classic), and uses the community-based security model of SNMPv1. In particular, SNMPv2c adds support for 64-bit counters.

- 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.

Tip We recommend using SNMPv3 wherever possible because of its superior security features.

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 (ACL) and password.

SNMPv2c support includes a retrieval mechanism and more detailed error message reporting to management stations. The 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. SNMPv1 reported all error conditions using a single error code, but SNMPv2c includes a number of expanded error codes that use different error types to distinguish between different kinds of error conditions.

SNMPv2 also reports three different types of exceptions:

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

SNMPv3

SNMPv3 improves security for SNMP communications by using encryption and by defining security models and security levels:

- Encryption—SNMPv3 supports several industry-standard encryption standards, including the Data Encryption Standard (DES).
- Security Model—An authentication strategy for a user and for the group in which the user resides. Different users can be assigned a different security model, depending on the organization's security structure and needs.
- Security Level—Permitted level of security within a security model. SNMPv1 and SNMPv2c used only a two-stage security level: read-only and read-write. SNMPv3 provides a much greater ability to customize the permission levels for different users.

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

Table 1-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	Description
v1	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v2c	noAuthNoPriv	Community string	No	Uses match on community string for authentication.
v3	noAuthNoPriv	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 SNMPv3.

Note We recommend using SNMPv3 for all SNMP applications, because of its significant security improvements. In addition, SNMPv3 supports 64-bit counters, which are not supported in SNMPv1. If you use SNMPv1, you can not view any objects that are defined as 64-bit counters.

Requests for Comments

MIB modules are typically defined in Request for Comments (**RFC**) documents that have been submitted to the Internet Engineering Task Force (IETF) for formal discussion and approval. 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 first 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.

Related Information and Useful Links

The following URLs provide access to general information about Cisco MIBs. Use these links to access MIBs for download, and to access related information (such as application notes and OID listings).

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

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

Cisco Technical Support Information and FAQs

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

- http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html is the Cisco Technical Support page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/en/US/customer/tech/tk648/tk362/technologies_q_and_a_item09186a0080094bc0.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.
- http://www.cisco.com/en/US/customer/tech/tk86/tk808/technologies_q_and_a_item09186a0080094cfd.shtml is a list of frequently asked questions (FAQs) about the use of SNMP on DOCSIS cable networks.

SNMP Configuration Information

The Cisco IOS Configuration Fundamentals and Network Management Configuration Guide, Release 12.3 at http://www.cisco.com/en/US/docs/ios/12_3/featlist/cfun_vcg.html provides information about configuring SNMP support and SNMP commands.

Cisco CMTS Documentation

The following documents describe information about configuring the cable-specific parameters on the Cisco CMTS router:

- *Cisco Broadband Cable Command Reference Guide,* at: http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
- *Cisco CMTS Feature Guide*, at the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/cmtsfg.html

Specifications and Standards

The following are standards and specifications that are used on DOCSIS cable networks. Some of these standards define the MIBs and other aspects of network management that are required for DOCSIS networks.

Note Many of these standards do not directly affect SNMP operations, but they define operational modes and parameters that must be understood to be able to interpret many of the tables and objects that are monitored and managed through SNMP.

Standards[1]	Title
DOCSIS Specifications—These specifications describe the operation and behavior of both CMTS and cable modem platforms on a DOCSIS cable network.	
ANSI/SCTE 22-1 200	Data-over-Cable Service Interface Specifications Radio Frequency Interface, version 1.0
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-RFIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0
SP-OSSIv2.0-I03-021218	Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0
SP-BPI+-I09-020830	Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0
CableHome Specifications—These specifications are not implemented on the CMTS platform but might be useful in understanding the behavior of cable modems and CPE devices.	
CH-SP-MIB-QOS-I03-040129	CableHome QOS MIB Specification
CH-SP-MIB-CAP-I05-040129	CableHome CAP MIB Specification
CH-SP-MIB-CDP-I05-040129	CableHome CDP MIB Specification
CH-SP-MIB-CTP-I05-040129	CableHome CTP MIB Specification
CH-SP-MIB-PSDEV-I05-040129	CableHome PSDEV MIB Specification
CH-SP-MIB-SEC-I05-040129	CableHome Security MIB Specification
CL-SP-MIB-CLABDEF-I03-040113	CableLabs Definition MIB Specification

1. Not all supported standards are listed.

CHAPTER 2

Configuring SNMP and MIB Support

This chapter describes how to configure Simple Network Management Protocol (SNMP) and Management Information Base (MIB) support for Cisco CMTS routers. It includes the following sections:

- Determining MIB Support for Cisco IOS Releases, page 2-1
- Downloading and Compiling MIBs, page 2-3
- Enabling SNMP Support, page 2-4
- High CPU Usage When Polling Routing ARP Tables, page 2-5
- Using SNMP MIBs in DOCSIS 3.0 Downstream Solution, page 2-7

Determining MIB Support for Cisco IOS Releases

Use one of the following procedures to determine which MIBs are included in the Cisco IOS release running on your router.

- Cisco MIBs Supported By Product, page 2-1
- Using the MIBs in Images Mail Service, page 2-2

Cisco MIBs Supported By Product

The Cisco MIBS Support page provides information on the SNMP capabilities that are contained in most Cisco IOS software images. To access this web site, use the following procedure:

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 your particular Cisco CMTS platform to display a list of MIBs that are supported on the router.

Step 3 Scroll through the list to find the Cisco IOS software release you are interested in.

Using the MIBs in Images Mail Service

The MIBs in Images (MII) mail service allows you to send an e-mail containing one or more Cisco IOS software images to a software database that is maintained by Cisco. The mail service checks the software database for the listed software images, and if it finds the images you supplied, it returns an e-mail to you with the list of MIBs that are supported in each software image.

To access the MII mail service, use the following procedure:

Step 1 Use the **show version** command to display the filename for the Cisco IOS image your router is running. The line that shows the filename starts with "System image file". For example, the following sample output shows that the Cisco IOS image filename is "`ubr7200-ik8s-mz.122-15.BC1.bin`".

```
Router# show version

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (UBR7200-IK8S-M), Version 12.2(15)BC1, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Mon 27-Mar-03 10:24 by cdei
Image text-base: 0x60008954, data-base: 0x6129C000

ROM: System Bootstrap, Version 12.2(1r) [dchjh 1r], RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (UBR7200-BOOT-M), Version 12.0(15)SC, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)

uptime is 1 week, 22 hours, 53 minutes
System returned to ROM by reload at 11:19:36 UTC Tue Jun 24 2003
System restarted at 11:21:08 UTC Tue Jun 24 2003
System image file is "slot0:ubr7200-ik8s-mz.122-15.BC1.bin"
```

Step 2 Send an e-mail to the e-mail address mii@external.cisco.com that includes the image filename by itself in the body of the e-mail text. (Do not include the location of the file, which could be a device name, such as "slot0:", or a TFTP URL.)

Step 3 After a few minutes, the MIBs in Images Mail service sends back an e-mail listing the MIBs contained in this particular Cisco IOS software release. (For more help on using the MIBs In Images mail service, send a blank e-mail to mii@external.cisco.com with the word "help" in the subject line.)

Tip You can also display an abbreviated list of the MIBs that are supported on a router running a particular Cisco IOS software release by logging in to the privileged EXEC prompt and giving the following command:

```
Router# show subsys | include mibs
```

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the router:

- Considerations for Working with MIBs, page 2-3
- Downloading MIBs, page 2-4
- Compiling MIBs, page 2-4

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, try loading 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

- To see a particular MIB's dependencies, use the "View and Download MIBs" tool, which is part of the SNMP Object Navigator on the Cisco IOS MIB Tools page, which is MIB Locator at the following URL:

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

- For information about trap definitions, alternative size definitions, and null OIDs, follow the link:

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

For listings of OIDs assigned to MIB objects, follow the link:

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

Downloading MIBs

To download the MIBs onto your system, if they are not already there, use the following procedure:

Step 1 Go to the Cisco IOS MIB Tools page at the following URL:

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

If the MIB you want to download is not there, try one of the URLs in Step 4.

Step 2 Click the link for the MIB Locator tool.

Step 3 You can use the MIB Locator tool to show a particular MIB or to show all MIBs for a particular platform or for a particular software release.

Step 4 You can also download industry-standard MIBs from the following URLs:

- http://www.ietf.org
- http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- http://www.broadband-forum.org/

Compiling MIBs

If you plan to integrate the Cisco CMTS with an SNMP-based management application, you must also compile the MIBs for that platform. Some SNMP managers do this automatically when you place all of the MIBs in a specific location, while others require you to do this manually. For instructions, see the documentation for that particular manager.

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco CMTS 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 If you plan to enable a number of traps, especially if you plan to enable traps for SYSLOG events and alarms, increase the trap queue size from its default of 10:

```
Router(config)# snmp-server queue-length queue-size
```

The value of *queue-size* can range from 1 to 1000 traps. We recommend a size of at least 100 for systems that are sending traps for SYSLOG events. The default is 10.

Step 5 See the "Enabling Notifications" section on page 4-2 for information on how to enable traps.

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

- "System Management" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.3, available at : http://www.cisco.com/en/US/docs/ios/12_3/featlist/cfun_vcg.html
- "System Management" section of the *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2, available at: http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html

High CPU Usage When Polling Routing ARP Tables

Using SNMP to poll large routing tables and Address Resolution Protocol (ARP) tables can cause performance problems on Cisco routers. This section provides background information about the issue, and how to avoid the problem.

An SNMP network management station can query a Cisco router to learn about other networks. The management station uses this routing information to find other routers and query them about the networks around them. This allows the management station to learn the topology of the entire network.

The router stores the routing table in hash format, which allows the router to quickly and efficiently search the table. However, RFC 1213 requires that SNMP return the routes in lexicographical order, which means they are listed by their OIDs, in the order in which they occur in the OID tree.

This means that for each SNMP request for routing information, the router must sort entries into the OID order before it builds the response protocol data unit (PDU). As the size of the routing table increases, the router must take a proportionately longer time, along with higher CPU processing levels, to sort the table entries.

Note The number of CPU cycles needed to respond to a request for the entire routing table depends on the size of the table (more routes require more CPU cycles). Therefore, even if your router does not currently exhibit CPU spikes, it might begin to do so as the size of the routing table increases.

To the CPU scheduler, SNMP is a low-priority process. This means that the CPU processes non-SNMP requests before it processes SNMP requests. Therefore, any CPU spikes that might occur during SNMP route polling should not affect router performance.

To avoid the performance problems that can occur when SNMP is used to retrieve the routing table or the ARP table, configure the router as described in either of the following sections:

- Enabling CEF Fast Switching on the Router, page 2-6
- Using snmp-server view Commands, page 2-6

For additional information on controlling SNMP traffic, see the application note, *IP Simple Network Management Protocol (SNMP) Causes High CPU Utilization,* at the following URL:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a00800948e6.shtml

Tip For information about other causes of high CPU usage, see the Cisco Technical Support document at the following URL:

Troubleshooting High CPU Utilization on Cisco Routers

Enabling CEF Fast Switching on the Router

To avoid the performance problems that can occur when SNMP GET-NEXT requests are used to retrieve the routing table or the ARP table, enable Cisco Express Forwarding (CEF) fast switching on the router. This is because the router processes SNMP requests differently, depending on whether fast switching is enabled:

- When fast switching is not enabled, the router uses information in the Routing Information Base (RIB) to respond to SNMP requests for the routing table or the ARP table. Entries in the RIB are not sorted by their **OID**, so the router must first sort these tables by their OID values, resulting in higher CPU usage.
- When fast switching is enabled, the router uses information in the Forwarding Information Base (FIB) to respond to SNMP requests for the routing table or the ARP table. FIB entries are stored in lexicographical order, listed by the router OID. Therefore, the router does not have to sort the routing tables before replying to SNMP requests, improving response time and reducing CPU usage.

Using snmp-server view Commands

Another way to avoid performance issues is to use SNMPv3 views to force the router to prematurely end queries for the route table and to respond instead with a “complete” message. Doing so blocks requests to retrieve the route table (ipRouteTable) and the ARP table (ipNetToMediaTable), but allows all other requests.

The following command example creates a view named cutdown that blocks requests for the route table and the ARP table, but allows all other requests. Note that you will need to substitute your own view name and community strings when you enter these commands on your router.

```
snmp-server view cutdown internet included
snmp-server view cutdown ipRouteTable excluded
snmp-server view cutdown ipNetToMediaTable excluded
snmp-server view cutdown at excluded
snmp-server community public view cutdown RO
snmp-server community private view cutdown RW
```

This configuration prevents the router from returning either the IP route table or the ARP table as part of an SNMP request. This prevents SNMP network discoveries from creating CPU spikes on the router, but it also removes a degree of manageability from the router.

Using SNMP MIBs in DOCSIS 3.0 Downstream Solution

Cisco IOS Release 12.3(21)BC and later releases support several MIBs on the Cisco uBR10012 router, Cisco shared port adaptor (SPA), and Cisco SPA interface processors (SIPs) for DOCSIS 3.0 Downstream Solution.

The following MIBs are supported in Cisco IOS Release 12.3(21)BC and later for the Cisco uBR10012 router and SIPs:

- ENTITY-MIB
- IF-MIB

The following MIBs are supported in Cisco IOS Release 12.3(21)BC and later for the Cisco uBR10012 router and the Wideband SPA:

- ENTITY-MIB
- CISCO-CABLE-WIDEBAND-MIB
- IF-MIB
- CISCO-VENDORTYPE-OID-MIB

Cisco IOS Release 12.3(23)BC introduces support for DOCSIS 3.0 Downstream Solution on the Cisco uBR10012 router and Cisco SIP and SPA. The following MIBs are introduced or enhanced further in Cisco IOS Release 12.3(23)BC for DOCSIS 3.0 Downstream Solution on the Cisco CMTS:

- CISCO-CABLE-SPECTRUM-MIB
- CISCO-CABLE-WIDEBAND-MIB
- CISCO-DOCS-EXT-MIB
- CISCO-VENDORTYPE-OID-MIB
- DOCS-DSG-IF-MIB
- DOCS-IF-MIB
- DTI-MIB
- DOCS-BPI-PLUS-MIB
- DOCS-CABLE-DEVICE-MIB
- DOCS-CABLE-DEVICE-TRAP-MIB
- ENTITY-MIB
- IF-MIB

Using the Cisco MIB Locator

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator found at the following URL:

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

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Additional References

Additional information is available in these separate documents on Cisco.com:

- *Cisco Cable Wideband Solution Design and Implementation Guide, Release 1.0*

  http://www.cisco.com/en/US/docs/cable/cmts/wideband/solution/guide/release_1.0/wb_solu.html

- *Cisco uBR10012 Universal Broadband Router SIP and SPA Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/uBR10012/hwsipspa.html

- *Cisco uBR10012 Universal Broadband Router SIP and SPA Software Configuration Guide*

  http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/configuration/ubr10012/12.3_23_bc/sipsp_d3.htmll

CHAPTER 3

MIB Specifications

This chapter describes each Management Information Base (MIB) on the Cisco CMTS router. Each description lists any constraints on how the MIB or its object identifiers (OIDs) are implemented on the router.

Unless noted otherwise, the Cisco CMTS implementation of a MIB follows the standard MIB that has been defined. Any MIB table or object not listed the tables is implemented as defined in the standard MIB definition.

Note Not all MIBs included in a Cisco IOS software 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. When a MIB is included in the image, this does not necessarily mean it is supported by the Cisco CMTS platform.

Note For information about how to avoid performance problems when you use Simple Network Management Protocol (SNMP) to poll the router for routing table entries, see the "High CPU Usage When Polling Routing ARP Tables" section on page 2-5.

Overview of MIB Support

Support for a particular MIB is included as part of the Cisco IOS software release. Each version of Cisco IOS software contains code that responds to SNMP requests for objects that are in the MIBs that are supported in that release for that particular software image.

Each new release of Cisco IOS software typically changes that support to some extent, usually involving one or more of the following:

- Fixing a caveat or software defect that is preventing the proper use of the MIB
- Updating the software to support the latest version of the MIB or to support optional objects that were not supported previously
- Adding support for new MIBs that are part of a new feature that is being introduced

The fact that a MIB might be included in a Cisco IOS software release does not imply that the MIB is fully supported on the router. Similarly, the fact that you can access a particular object in a MIB does not imply that the object is fully supported either.

Note As a general rule, deprecated objects and MIBs should not be used, because they have been replaced by other, more functional objects and MIBs. Also, deprecated objects and MIBs can be removed in a future release without notice.

Note The exact MIB support depends on both the Cisco IOS software image and the Cisco IOS software release being used. To determine which MIBs are included in other releases and software images, see the "Determining MIB Support for Cisco IOS Releases" section on page 2-1.

Table 3-1 lists the MIBs that are included in Cisco IOS Release 12.3BC for Cisco CMTS routers, through Cisco IOS Release 12.3(23)BC. Shaded cells indicate that the MIB is not included for that particular platform and software release. 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.

Table 3-1 Included MIBs on Cisco uBR10012 and uBR7200 Series Routers in Cisco IOS Release 12.3(23)BC

Cisco uBR7200 series in Cisco IOS Release 12.3(23)BC	Cisco uBR10012 Cisco IOS Release 12.3(23)BC
ATM-MIB	ATM-MIB
BGP4-MIB	BGP4-MIB
BRIDGE-MIB (-is- software images only)	
CISCO-AAA-SERVER-MIB	CISCO-AAA-SERVER-MIB
CISCO-AAL5-MIB	CISCO-AAL5-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-ACCESS-ENVMON-MIB
CISCO-ATM-EXT-MIB	CISCO-ATM-EXT-MIB
CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-ATM-PVCTRAP-EXTN-MIB
CISCO-BGP4-MIB	CISCO-BGP4-MIB
CISCO-BULK-FILE-MIB (-is- software images only)	CISCO-BULK-FILE-MIB
CISCO-BUS-MIB (-is- software images only)	
CISCO-CABLE-ADMISSION-CTRL-MIB	CISCO-CABLE-ADMISSION-CTRL-MIB
CISCO-CABLE-AVAILABILITY-MIB	CISCO-CABLE-AVAILABILITY-MIB
CISCO-CABLE-METERING-MIB	CISCO-CABLE-METERING-MIB
CISCO-CABLE-QOS-MONITOR-MIB	CISCO-CABLE-QOS-MONITOR-MIB
CISCO-CABLE-SPECTRUM-MIB	CISCO-CABLE-SPECTRUM-MIB
	CISCO-CABLE-WIDEBAND-MIB
CISCO-CAR-MIB	CISCO-CAR-MIB
CISCO-CASA-FA-MIB (-is- software images only)	

Table 3-1 Included MIBs on Cisco uBR10012 and uBR7200 Series Routers in Cisco IOS Release 12.3(23)BC

Cisco uBR7200 series in Cisco IOS Release 12.3(23)BC	Cisco uBR10012 Cisco IOS Release 12.3(23)BC
CISCO-CASA-MIB (-is- software images only)	
CISCO-CDP-MIB	CISCO-CDP-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-CIRCUIT-INTERFACE-MIB
CISCO-CLASS-BASED-QOS-MIB	
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB	
CISCO-CONFIG-COPY-MIB	CISCO-CONFIG-COPY-MIB
CISCO-CONFIG-MAN-MIB	CISCO-CONFIG-MAN-MIB
CISCO-DOCS-EXT-MIB	CISCO-DOCS-EXT-MIB
CISCO-DOCS-REMOTE-QUERY-MIB	
	CISCO-ENHANCED-MEMPOOL-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-ENTITY-ALARM-MIB
CISCO-ENTITY-ASSET-MIB	CISCO-ENTITY-ASSET-MIB
CISCO-ENTITY-EXT-MIB	CISCO-ENTITY-EXT-MIB
CISCO-ENTITY-FRU-CONTROL-MIB	CISCO-ENTITY-FRU-CONTROL-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-ENTITY-VENDORTYPE-OID-MIB
CISCO-ENVMON-MIB	
CISCO-FLASH-MIB	CISCO-FLASH-MIB
CISCO-FRAME-RELAY-MIB	CISCO-FRAME-RELAY-MIB
CISCO-FTP-CLIENT-MIB (-is- software images only)	CISCO-FTP-CLIENT-MIB
CISCO-HSRP-EXT-MIB	CISCO-HSRP-EXT-MIB
CISCO-HSRP-MIB	CISCO-HSRP-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-IETF-ATM2-PVCTRAP-MIB
CISCO-IETF-IP-FORWARD-MIB	
CISCO-IETF-IP-MIB	
CISCO-IETF-NAT-MIB (-is- software images only)	
CISCO-IMAGE-MIB	CISCO-IMAGE-MIB
CISCO-IPMROUTE-MIB	CISCO-IPMROUTE-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-FLOW-MONITOR-MIB
CISCO-IPSEC-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-MIB
CISCO-IPSEC-POLICY-MAP-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-POLICY-MAP-MIB
CISCO-IP-STAT-MIB	CISCO-IP-STAT-MIB

Table 3-1 Included MIBs on Cisco uBR10012 and uBR7200 Series Routers in Cisco IOS Release 12.3(23)BC

Cisco uBR7200 series in Cisco IOS Release 12.3(23)BC	Cisco uBR10012 Cisco IOS Release 12.3(23)BC
CISCO-ISDN-MIB	
CISCO-LEC-DATA-VCC-MIB (-is- software images only)	
CISCO-LEC-EXT-MIB (-is- software images only)	
CISCO-LECS-MIB (-is- software images only)	
CISCO-LES-MIB (-is- software images only)	
CISCO-MEMORY-POOL-MIB	CISCO-MEMORY-POOL-MIB
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	
CISCO-NTP-MIB	CISCO-NTP-MIB
CISCO-PIM-MIB	CISCO-PIM-MIB
CISCO-PING-MIB	CISCO-PING-MIB
CISCO-PPPOE-MIB	
CISCO-PROCESS-MIB	CISCO-PROCESS-MIB
CISCO-PRODUCTS-MIB	CISCO-PRODUCTS-MIB
CISCO-QUEUE-MIB	CISCO-QUEUE-MIB
CISCO-RMON-SAMPLING-MIB	CISCO-RMON-SAMPLING-MIB
CISCO-RTTMON-MIB	CISCO-RTTMON-MIB
CISCO-SNAPSHOT-MIB	CISCO-SNAPSHOT-MIB
	CISCO-SRP-MIB
CISCO-SYSLOG-MIB	CISCO-SYSLOG-MIB
CISCO-TCP-MIB	CISCO-TCP-MIB
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB
CISCO-VPDN-MGMT-MIB (-is- software images only)	
CISCO-VPDN-MGMT-EXT-MIB (-is- software images only)	
CISCO-VSIMASTER-MIB	
DOCS-BPI-MIB (-k8- or -k9- software images only)	DOCS-BPI-MIB
DOCS-BPI-PLUS-MIB (-k8- or -k9- software images only)	DOCS-BPI-PLUS-MIB Narrowband fiber nodes and Multicast supported in Cisco IOS Release 12.3(23)BC and later.
DOCS-CABLE-DEVICE-MIB	DOCS-CABLE-DEVICE-MIB
DOCS-CABLE-DEVICE-TRAP-MIB	DOCS-CABLE-DEVICE-TRAP-MIB
DOCS-DSG-IF-MIB	DOCS-DSG-IF-MIB

Table 3-1 Included MIBs on Cisco uBR10012 and uBR7200 Series Routers in Cisco IOS Release 12.3(23)BC

Cisco uBR7200 series in Cisco IOS Release 12.3(23)BC	Cisco uBR10012 Cisco IOS Release 12.3(23)BC
DOCS-IF-MIB	DOCS-IF-MIB
DOCS-IF-EXT-MIB	DOCS-IF-EXT-MIB
DOCS-QOS-MIB	DOCS-QOS-MIB
	DTI-MIB
ENTITY-MIB	ENTITY-MIB*
ETHERLIKE-MIB	ETHERLIKE-MIB
EVENT-MIB (-is- software images only)	EVENT-MIB
EXPRESSION-MIB (-is- software images only)	EXPRESSION-MIB
HC-RMON-MIB	HC-RMON-MIB
IF-MIB	IF-MIB
IGMP-STD-MIB	IGMP-STD-MIB
INT-SERV-MIB	INT-SERV-MIB
IP-MIB	IP-MIB
IPMROUTE-STD-MIB	IPMROUTE-STD-MIB
ISDN-MIB	
LAN-EMULATION-CLIENT-MIB (-is- software images only)	
MSDP-MIB	MSDP-MIB
NOTIFICATION-LOG-MIB (not supported in -is- software images)	
	nruCacheSnmpData
OLD-CISCO-CHASSIS-MIB	OLD-CISCO-CHASSIS-MIB
OLD-CISCO-CPU-MIB	OLD-CISCO-CPU-MIB
OLD-CISCO-INTERFACES-MIB	OLD-CISCO-INTERFACES-MIB
OLD-CISCO-IP-MIB	OLD-CISCO-IP-MIB
OLD-CISCO-MEMORY-MIB	OLD-CISCO-MEMORY-MIB
OLD-CISCO-SYSTEM-MIB	OLD-CISCO-SYSTEM-MIB
OLD-CISCO-TCP-MIB	OLD-CISCO-TCP-MIB
OLD-CISCO-TS-MIB	OLD-CISCO-TS-MIB
PIM-MIB	PIM-MIB
RFC1213-MIB	RFC1213-MIB
RFC1231-MIB	
RFC1253-MIB	RFC1253-MIB
RFC1315-MIB	RFC1315-MIB
RFC1381-MIB	
RFC1382-MIB	

Table 3-1 Included MIBs on Cisco uBR10012 and uBR7200 Series Routers in Cisco IOS Release 12.3(23)BC

Cisco uBR7200 series in Cisco IOS Release 12.3(23)BC	Cisco uBR10012 Cisco IOS Release 12.3(23)BC
RFC1406-MIB	RFC1406-MIB
RFC1407-MIB	RFC1407-MIB
RFC1595-MIB	RFC1595-MIB
RMON-MIB	RMON-MIB
RMON2-MIB	RMON2-MIB
RS-232-MIB	RS-232-MIB
RSVP-MIB	RSVP-MIB
SMON-MIB	SMON-MIB
SNMP-COMMUNITY-MIB	SNMP-COMMUNITY-MIB
SNMP-FRAMEWORK-MIB	SNMP-FRAMEWORK-MIB
SNMP-MPD-MIB	
SNMP-NOTIFICATION-MIB	SNMP-NOTIFICATION-MIB
SNMP-PROXY-MIB	SNMP-PROXY-MIB
SNMP-TARGET-MIB	SNMP-TARGET-MIB
SNMP-USM-MIB	SNMP-USM-MIB
SNMPv2-MIB	SNMPv2-MIB
SNMP-VACM-MIB	SNMP-VACM-MIB
TCP-MIB	TCP-MIB
UDP-MIB	UDP-MIB

Table 3-2 list the specific cable MIBs.

Table 3-2 Cable-Specific MIBs

MIB Name	MIB Description
DOCS-IF-MIB	Describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems and the CMTS. This MIB has been released as an RFC 2670.
DOCS-BPI-PLUS-MIB	Describes the attributes for the DOCSIS 1.1-specified Baseline Privacy Interface Plus (BPI+) on CMS and the CMTS. This is a draft revision 05 of the MIB. **Note** This MIB replaces DOCS-BPI-MIB, which was used in the initial DOCSIS 1.0 releases.
CISCO-DOCS-EXT-MIB	Extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as Quality of Service (QoS) attributes and connection status and other information regarding the cable modems and Customer Premise Equipment (CPE) devices supported by the CMTS.
CISCO-DOCS-REMOTE-QUERY-MIB	Facilitates SNMP polling of remote cable modems on CMTS.

Table 3-2 Cable-Specific MIBs

MIB Name	MIB Description
CISCO-CABLE-SPECTRUM-MIB	Describes the spectrum management and flap list attributes.
CISCO-CABLE-ADMISSION-CTRL-MIB	Enables the management of Cable Modem Termination System (CMTS) admission control.
CISCO-CABLE-AVAILABILITY-MIB	Describes the operation of Hot Standby Connection to Connection Protocol (HCCP) N+1 redundancy on the Cisco CMTS.
CISCO-CABLE-METERING-MIB	Describes subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, also known as Usage-Based Billing on the Cisco CMTS.
CISCO-CABLE-QOS-MONITOR-MIB	Describes SNMP support for the Subscriber Traffic Management (STM) feature.
DOCS-QOS-MIB	Describes the QoS attributes. This is a draft revision 05 of the MIB. **Note** Cisco IOS Software Release 12.1(4)CX implemented revision 02 of this MIB. Revision 05 includes substantial changes to the tables and attributes.
DOCS-SUBMGT-MIB	Describes the subscriber management attributes. This is revision 02 of the MIB.
IGMP-STD-MIB	Describes the Internet Group Management Protocol (IGMP) attributes, as defined in RFC 2933.
DOCS-CABLE-DEVICE-MIB	Describes the operation of cable modem and CMTS. Only the syslog and Event tables are supported by this MIB, which was released as RFC 2669.
DOCS-CABLE-DEVICE-TRAP-MIB	This is the extension of the RFC2669 (DOCS-CABLE-DEVICE-MIB). It defines all the traps supported by a cable modem and CMTS.
CISCO-CABLE-WIDEBAND-MIB	Contains objects that support Wideband DOCSIS on the Cable Modem Termination System (CMTS).

MIB Specifications

This section gives a short summary of each MIB, along with the MODULE-IDENTITY and top-level object identifier (OID) that can be used to access the MIB when using an SNMP manager.

ATM-MIB

The ATM-MIB contains the Asynchronous Transfer Mode (ATM) and ATM adaptation layer 5 (AAL5) objects used to manage ATM interfaces, virtual links, cross connects, and AAL5 entities and connections, as defined in RFC 1695.

The MODULE-IDENTITY for the ATM-MIB is atmMIB, and its top-level OID is 1.3.6.1.2.1.37 (iso.org.dod.internet.mgmt.mib-2.atmMIB).

MIB Constraints

There are no constraints on this MIB.

BGP4-MIB

The BGP4-MIB provides access to information related to the implementation of the Border Gateway Protocol (BGP), as defined in RFC 1657. The MIB provides:

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

The MODULE-IDENTITY for the BGP4-MIB is bgp, and its top-level OID is 1.3.6.1.2.1.15 (iso.org.dod.internet.mgmt.mib-2.bgp).

MIB Constraints

There are no constraints on this MIB.

BRIDGE-MIB

The BRIDGE-MIB provides access to information related to Layer 2 bridging that is based on MAC addresses, as defined in RFC 1493.

The MODULE-IDENTITY for the BRIDGE-MIB is dot1dBridge, and its top-level OID is 1.3.6.1.2.1.17 (iso.org.dod.internet.mgmt.mib-2.dot1dBridge).

MIB Constraints

This MIB is supported only on the Cisco uBR7100 series router when running a Cisco IOS “-is-” software image. It is not supported on the Cisco uBR7200 series and Cisco uBR10012 routers, which do not support bridging across cable interfaces.

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 casConfigTable are implemented as read-only.

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

MIB Object	Notes
casConfigTable	
• casAddress	Read-only.
• casAuthenPort	Read-only.
• casAcctPort	Read-only.
• casKey	Read-only.
• casConfigRowStatus	Read-only.

CISCO-AAL5-MIB

The CISCO-AAL5-MIB contains performance statistics for ATM adaptation layer 5 (AAL5) virtual channel connections (VCCs). This MIB provides additional statistics that supplement the information stored in the aal5VccTable in ATM-MIB (RFC 1695), such as packets and octets received and transmitted on the VCC.

The MODULE-IDENTITY for the CISCO-AAL5-MIB is ciscoAal5MIB, and its top-level OID is 1.3.6.1.4.1.9.9.66 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoAal5MIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-ACCESS-ENVMON-MIB

The CISCO-ACCESS-ENVMON-MIB supplements the ciscoEnvMonSupplyStatusTable table in CISCO-ENVMON-MIB, providing additional information about power supply failures. This MIB also defines new temperature and voltage notifications that replace those in CISCO-ENVMON-MIB.

The MODULE-IDENTITY for the CISCO-ACCESS-ENVMON-MIB is ciscoAccessEnvMonMIB, and its top-level OID is 1.3.6.1.4.1.9.9.61 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoAccessEnvMonMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-ATM-EXT-MIB

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

The MODULE-IDENTITY for the CISCO-ATM-EXT-MIB is ciscoAtmExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.88 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoAtmExtMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-ATM-PVCTRAP-EXTN-MIB

The CISCO-ATM-PVCTRAP-EXTN-MIB contains extensions to the ATM-MIB, providing additional notifications and traps about the status of permanent virtual circuits (PVCs) on the Cisco CMTS.

The MODULE-IDENTITY for the CISCO-ATM-PVCTRAP-EXTN-MIB is ciscoAtmPvcTrapExtnMIB, and its top-level OID is 1.3.6.1.4.1.9.10.97 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoAtmPvcTrapExtnMIB).

MIB Constraints

The CISCO-ATM-PVCTRAP-EXTN-MIB has the following constraints.

Table 3-4 CISCO-ATM-PVCTRAP-EXTN-MIB Constraints

This is an experimental MIB that can be obsoleted and replaced without prior notice.
This MIB is not supported in any Cisco IOS Release 12.1EC software image

CISCO-BGP4-MIB

The CISCO-BGP4-MIB contains extensions to the BGP4-MIB that are specific to Cisco, including additional information about the entries in the BGP routing table.

The MODULE-IDENTITY for the CISCO-BGP4-MIB is ciscoBgp4MIB, and its top-level OID is 1.3.6.1.4.1.9.9.187 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoBgp4MIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-BGP-POLICY-ACCOUNTING-MIB

The CISCO-BGP-POLICY-ACCOUNTING-MIB contains objects for BGP policy-based accounting that are specific to Cisco platforms.

The MODULE-IDENTITY for the CISCO-BGP-POLICY-ACCOUNTING-MIB is ciscoBgpPolAcctMIB, and its top-level OID is 1.3.6.1.4.1.9.9.148 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoBgpPolAcctMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers.
- This MIB is not supported on Cisco uBR10012 routers.
- This MIB is not supported in Cisco IOS Release 12.2BC.

CISCO-BULK-FILE-MIB

The CISCO-BULK-FILE-MIB contains objects to create and delete files of SNMP data for bulk-file transfer, in different file formats (ASN.1/BER, binary, and ASCII).

The MODULE-IDENTITY for the CISCO-BULK-FILE-MIB is ciscoBulkFileMIB, and its top-level OID is 1.3.6.1.4.1.9.9.81 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoBulkFileMIB).

MIB Constraint

This MIB is supported only on Cisco uBR7100 series and Cisco uBR7200 series routers that are running a Cisco IOS “-is-” software image.

CISCO-BUS-MIB

The CISCO-BUS-MIB contains objects about the operation of each broadcast and unknown server (BUS) that is operating on an ATM virtual LAN (VLAN) that is using LAN Emulation (LANE) tagging.

The MODULE-IDENTITY for the CISCO-BUS-MIB is ciscoBusMIB, and its top-level OID is 1.3.6.1.4.1.9.9.40 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoBusMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is supported only on Cisco uBR7100 series and Cisco uBR7200 series routers that are running a Cisco IOS “-is-” software image.
- This MIB is not supported on the Cisco uBR10012 router.

CISCO-CABLE-ADMISSION-CTRL-MIB

The CISCO-CABLE-ADMISSION-CTRL-MIB contains objects enabling the management of Cable Modem Termination System (CMTS) admission control. Admission Control refers to the rules that the Cisco CMTS follows when allocating and monitoring events for resources such as the following:

- CPU and memory utilization—Data and thresholds setting on the physical entity, such as the main processor or line card or Broadband processing Engines (BPE), when a monitoring event happens
- Configuration of thresholds and channel bandwidth utilization, both Upstream (US) and Downstream (DS), are based on application types

The monitored events for Admission Control on the Cisco CMTS include the following:

- Dynamic service flow creation requests—Dynamic service flow allows on-demand reservation on Layer 2 bandwidth resources. CMTS provides special QoS to the cable modem dynamically during a voice call or video session which provides a more efficient use of the available bandwidth.
- Resource requests during cable modem (CM) registration—CMTS resources are required during CM registration. CMTS resources are checked when CM receives a registration request.

Note For detailed information about admission control for Cisco CMTS, go to the following URL: http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_adm.html

MIB Constraints

This MIB has the following constraints.

Table 3-5 CISCO-CABLE-ADMISSION-CTRL-MIB Constraints

MIB Object	Notes
ccacEventHistTable	
• ccacEventHistTableSize	The ccacEventHistTableSize object specifies the number of entries that the ccacEventHistTable can contain. When the capacity of the ccacEventHistTable has reached the value specified by this object, then the agent deletes the oldest entity in order to accommodate the new entry. A value of zero prevents any history from being retained. The ccacEventHistTableSize is restricted to 5000.
• ccacSysRscConfigStatus	Read-only.

CISCO-CABLE-AVAILABILITY-MIB

The CISCO-CABLE-AVAILABILITY-MIB contains objects about the operation of Hot Standby Connection to Connection Protocol (HCCP) N+1 redundancy on the Cisco CMTS.

The MODULE-IDENTITY for the CISCO-CABLE-AVAILABILITY-MIB is ciscoCableAvailabilityMIB, and its top-level OID is 1.3.6.1.4.1.9.9.242 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCableAvailabilityMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is not supported in any Cisco IOS Release 12.1EC software image.
- This MIB is not supported on the Cisco uBR7100 series router.
- This MIB is supported on the Cisco uBR10012 router in Cisco IOS Release 12.2(8)BC1 and later releases.

CISCO-CABLE-METERING-MIB

The CISCO-CABLE-METERING-MIB contains objects that provide subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format, also known as Usage-Based Billing on the Cisco CMTS. This format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

The MODULE-IDENTITY for the CISCO-CABLE-METERING-MIB is ciscoCableMeteringMIB, and its top-level OID is 1.3.6.1.4.1.9.9.424 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCableMeteringMIB).

Note For complete documentation about using the Usage-Based Billing feature for Cisco CMTS, go to: http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html

MIB Constraints

This MIB has the following constraints:

- The packet counters displayed by CLI commands are reset to zero whenever the Cisco CMTS router is rebooted. The packet counters displayed by SNMP commands are retained across router resets. These counters are 64-bit values and could roll over to zero during periods of heavy usage.
- This MIB is supported only in Cisco IOS Release 12.3(9a)BC and later releases.

CISCO-CABLE-QOS-MONITOR-MIB

The CISCO-CABLE-QOS-MONITOR-MIB provides SNMP support for the Subscriber Traffic Management (STM) feature, which allows network administrators to identify users who violate their service level agreements (SLA) by using resources beyond their allowable bandwidth.

This MIB provides configuration options similar to those provided by the **cable qos enforce-rule** command. It also provides access to the attributes that are displayed by the **show cable qos enforce-rule** and **show cable subscriber-usage** commands.

The MODULE-IDENTITY for the CISCO-CABLE-QOS-MONITOR-MIB is ciscoCableQosMonitorMIB, and its top-level OID is 1.3.6.1.4.1.9.9.341 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCableQosMonitorMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is not supported in any Cisco IOS Release 12.1EC software image.
- This MIB is supported starting with Cisco IOS Release 12.2(15)BC1 and later releases.

CISCO-CABLE-SPECTRUM-MIB

The CISCO-CABLE-SPECTRUM-MIB provides SNMP support for spectrum management and flap-list operations on the Cisco CMTS.

Spectrum management is a feature provided in the CMTS so that the CMTS may identify both downstream and upstream plant impairments, report them to a management entity, and automatically diminish them where possible.

The purpose of cable spectrum management is to:

- Prevent long-term service interruptions caused by upstream noise events in the cable plant
- Provide fault management and troubleshooting on the cable network. The following new tables and objects are supported in this MIB:
  - ccsSpecGroupFreqTable
  - ccsUpInSpecGroupTable
  - ccsUpInCombGroupTable
  - ccsUpSpecMgmtSpecGroup
  - ccsUpSpecMgmtSharedSpectrum

The MODULE-IDENTITY for the CISCO-CABLE-SPECTRUM-MIB is ciscoCableSpectrumMIB, and its top-level OID is 1.3.6.1.4.1.9.9.114 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCableSpectrumMIB).

MIB Constraints

This MIB has the following constraints.

Table 3-6 CISCO-CABLE-SPECTRUM-MIB Constraints

MIB Object	Notes
ccsUpSpecMgmtTable	
• ccsUpSpecMgmtSNR	This object returns zero (0) in three situations: when the actual signal-to-noise ratio (SNR) measures 0 (when ingress noise cancellation is being used), when no cable modems are online the upstream, or when the SNMP agent on the router could not determine a valid SNR value.
• ccsUpSpecMgmtSpecGroup	Read-only. The value of 0 for this object indicates that the upstream has no spectrum group assigned to it.

Table 3-6 CISCO-CABLE-SPECTRUM-MIB Constraints (continued)

MIB Object	Notes
• ccsUpSpecMgmtSharedSpectrum	Read-only. The combiner group assigned to the upstream. Note: Upstreams having same combiner group number indicates that they physically combine together into the same RF domain and must have unique frequency assigned. The value of 0 for the object indicates that the upstream is not physically combine with any others.
ccsCmFlapTable	
• ccsFlapAging ccsFlapListMaxSize ccsFlapInsertionTime ccsFlapMissThreshold ccsFlapPowerAdjustThreshold ccsFlapResetAll, ccsFlapClearAll ccsFlapResetNow	These objects are supported on the Cisco uBR10012 router in Cisco IOS Release 12.2(11)BC3 and later releases. Commencing in Cisco IOS Release 12.3(23)BC, This table keeps the records of modem state changes, and can be used to identify problematic cable modems. The system automatically adds an entry per modem to the table when it detects any state changes to the modem. This table can be deleted but cannot be added by the management system.
• The following objects are supported in Cisco IOS release 12.3(23)BC and later releases: ccsCmFlapDownstreamIfIndex ccsCmFlapUpstreamIfIndex ccsCmFlapMacAddr	The index objects are ccsCmFlapDownstreamIfIndex, ccsCmFlapUpstreamIfIndex, ccsCmFlapMacAddr. This table is used to replace ccsFlapTable, using downstream, upstream and MAC address as indices for the flapped modem. For NB CMs using SPA Downstream, ccsCmFlapDownstreamIfIndex should be the ifindex of Modular Cable Interface's snmp ifindex.

MIB Group Objects

Table 3-7 lists the groups and objects added to the CISCO-CABLE-SPECTRUM-MIB.

Table 3-7 CISCO-CABLE-SPECTRUM-MIB Group Objects

MIB Object	Notes
ccsSpecGroupFreqTable	Contains the frequency and band configuration of the spectrum group.
• ccsSpecGroupNumber	
• ccsSpecGroupFreqIndex	Unsigned32
• ccsSpecGroupFreqType	INTEGER
• ccsSpecGroupFreqLower	Unsigned32
• ccsSpecGroupFreqUpper	Unsigned32
• ccsSpecGroupStorage	StorageType
• ccsSpecGroupRowStatus	RowStatus

Table 3-7 CISCO-CABLE-SPECTRUM-MIB Group Objects (continued)

MIB Object	Notes
ccsUpInSpecGroupTable	Contains the cable upstream interfaces assigned to a spectrum group. A spectrum group contains one or more fixed frequencies or frequency bands which can be assigned to cable upstream interfaces in the spectrum group.
• ccsSpecGroupNumber	Unsigned32
• ccsSpecGroupUpstreamIfIndex	InterfaceIndex
• ccsSpecGroupUpstreamStorage	StorageType
• ccsSpecGroupUpstreamRowStatus	RowStatus
ccsUpInCombGroupTable	Contains all the cable upstream interfaces in a combiner group. Each combiner group uniquely represents a RF domain. Cable upstream interfaces in same combiner group are physically combined together into same RF domain
• ccsCombGroupNumber	Unsigned32
• ccsCombGroupUpstreamIfIndex	InterfaceIndex
• ccsCombGroupUpstreamStorage	StorageType
• ccsCombGroupUpstreamRowStatus	RowStatus

CISCO-CABLE-WIDEBAND-MIB

CISCO-CABLE-WIDEBAND-MIB in Cisco IOS 12.3(21)BC

The CISCO-CABLE-WIDEBAND-MIB contains objects that support Channel Bonding Protocol for the Cable Modem Termination System (CMTS). Cisco Cable Wideband MIB supports Wideband DOCSIS on the Cable Modem Termination System (CMTS). Wideband DOCSIS enhances per-cable-modem data rates that exceed the bandwidth of a single 256QAM downstream channel.

The MODULE-IDENTITY for the CISCO-CABLE-WIDEBAND-MIB is ciscoCableWidebandMIBObjects, and its top-level OID is 1.3.6.1.4.1.9.9.479.

A wideband channel or Bonded Group is a logical grouping of one or more physical RF channels over which MPEG-TS packets are carried. The wideband channel carries DOCSIS-bonded packets encapsulated in MPEG-TS packets from a wideband Cisco CMTS to one or more wideband cable modems.

Narrowband and Wideband Channels in Cisco IOS 12.3(23)BC

Commencing in Cisco IOS Release 12.3(23)BC and later releases, the Cisco CMTS supports a narrowband channel in a standard DOCSIS downstream channel containing exactly one RF channel. The fiber node in a narrowband channel is an optical node that terminates the fiber-based downstream signal as an electrical signal onto a coaxial RF cable. This type of narrowband channel is distinct from another new narrowband channel that applies to the Shared Port Adaptor (SPA) downstream channel.

Narrowband in Cisco IOS 12.3(23)BC has been enhanced to support two tables in the CISCO-CABLE-WIDEBAND-MIB:

- ccwbWBtoRFMappingTable
- ccwbWBtoNBMappingTable

These MIB objects correspond to the two following privileged EXEC commands:

- **show hw-module bay all mapping wideband-channel**
- **show hw-module bay all association wideband-channel**

MIB Notes and Constraints

The CISCO-CABLE-WIDEBAND-MIB has the following constraints.

Table 3-8 CISCO-CABLE-WIDEBAND-MIB Constraints

MIB Object	Notes and Constraints
ccwbRFChannelTable	This table contains attributes of the physical RF channels.
• ccwbRFChannelFrequency	Unsigned32 Note: A range of 54MHz to 860MHz is appropriate for a cable plant using a North American Sub-Split channel plan. The spectrum range has been expanded to accommodate a lower edge of 47MHz and an upper edge of 862MHz for some European channel plants.
• ccwbRFChannelWidth	Read-only. Note: The value of 6 MHz is appropriate for cable plants running under NTSC (National Television Standards Committee) standards. The value of 8 MHz is appropriate for cable plants running under ETSI standards.
• ccwbRFChannelRowStatus	Values: • active(1) • createAndGo(4) • destroy(6)
• ccwbRFChannelAnnex	Read-create. Value must be the same for all RF channels.
• ccwbRFChannelModulation	Read-create. Value must be the same for all RF channels.
• ccwbRFChannelStorageType	Value is volatile(2).
• ccwbRFChannelNum	Unsigned32
• ccwbRFChannelMpegPkts	Read-only. Counter64
ccwbRFChannelQamTable	This table contains information of the external edge QAM which provide the physical RF channels which are available to the wideband channels.
• ccwbRFChanQamTos	Not implemented.
• ccwbRFChanQamVlanId	Not implemented.
• ccwbRFChanQamPriorityBits	Not implemented.
• ccwbWBtoNBRowStatus	Read-only.
• ccwbWBtoNBStorageType	Values: • volatile(2). • Read-only.

Table 3-8 CISCO-CABLE-WIDEBAND-MIB Constraints (continued)

MIB Object	Notes and Constraints
• ccwbRFChanQamIPAddressType	Only Internet address type **ipv4** is supported.
ccwbWBtoRFMappingTable	This table contains association information of the wideband channels to RF channels available for WCMTS. This converts to a Read-only table.
• ccwbWBtoRFStorageType	Value is volatile(2).
• ccwbWBtoRFRowStatus	Values: • active(1) • createAndGo(4) • destroy(6)
ccwbFiberNodeDescrTable	This table contains the description of a fiber node on a CMTS.
• ccwbFiberNodeDescription	Read-only.
• ccwbFiberNodeDescrStorageType	Values: • volatile(2). • Read-only.
• ccwbFiberNodeDescrRowStatus	Read-only.
ccwbFiberNodeTable	This is a read-only table which provides configuration and topology information for each Fiber node, such as, Narrowband Ifindex, Wideband controller Index and the Wideband rf-ports
• ccwbFiberNodeNBIfIndx	Read-only.
• ccwbFiberNodeWBContlrPhyIndx	Read-only.
• ccwbFiberNodeWBRFPort	Read-only.
• ccwbFiberNodeStorageType	Values: • volatile(2). • Read-only.
• ccwbFiberNodeRowStatus	Read-only.
ccwbWBCmStatusTable	This table contains wideband cable connectivity status .
• ccwbWBCmStatusValue	Read-only.
ccwbWBBondGrpTable	This table provides information on either a primary or non-primary interface for the Wideband Interface.
• ccwbWBBondGrpSecondary	Values: • true(1) if the wideband interface (BG) is Secondary • false(2) for non-secondary

Table 3-8 CISCO-CABLE-WIDEBAND-MIB Constraints (continued)

MIB Object	Notes and Constraints
ccwbWBtoRFMappingTable	This table maps the Wideband Fiber Node and associated interfaces to the RF downstream. This table is supported only in Cisco IOS Release 12.3(23)BC or later on the Cisco uBR10012 router. This MIB table corresponds to the **show hw-module bay all mapping wideband-channel** privileged EXEC command.
ccwbWBtoNBMappingTable	This table maps the Wideband interfaces to the Narrowband Fiber Node for downstream channels. This table is supported only in Cisco IOS Release 12.3(23)BC or later on the Cisco uBR10012 router. This MIB table corresponds to the **show hw-module bay all association wideband-channel** privileged EXEC command.
This is a Cisco-only proprietary MIB which supports the DOCSIS 3.0 standard.	

CISCO-CALL-HISTORY-MIB

The CISCO-CALL-HISTORY-MIB contains objects about the information that is stored in the router's call history table, which keeps a record of the calls made on the router.

The MODULE-IDENTITY for the CISCO-CALL-HISTORY-MIB is ciscoCallHistoryMib, and its top-level OID is 1.3.6.1.4.1.9.9.27 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCallHistoryMib).

MIB Constraints

This MIB is not supported on the Cisco uBR10012 router.

CISCO-CAR-MIB

The CISCO-CAR-MIB contains objects that provide information about the operation of packet filtering on the interfaces that use weighted rate-limiting, which is also known as the committed access rate (CAR).

The MODULE-IDENTITY for the CISCO-CAR-MIB is ciscoCarMIB, and its top-level OID is 1.3.6.1.4.1.9.9.113 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCarMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-CASA-FA-MIB

The CISCO-CASA-FA-MIB supplements the CISCO-CASA-MIB, containing additional objects to manage a Cisco Appliance Services Architecture (CASA) forwarding agent (FA).

The MODULE-IDENTITY for the CISCO-CASA-FA-MIB is ciscoCasaFaMIB, and its top-level OID is 1.3.6.1.4.1.9.9.115 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCasaFaMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is supported only on Cisco uBR7100 series and Cisco uBR7200 series routers that are running a Cisco IOS "-is-" software image.
- This MIB is not supported on the Cisco uBR10012 router.

CISCO-CASA-MIB

The CISCO-CASA-MIB contains the objects needed to manage a Cisco Appliance Services Architecture (CASA) entity, which can be either a manager agent or forwarding agent.

The MODULE-IDENTITY for the CISCO-CASA-MIB is ciscoCasaMIB, and its top-level OID is 1.3.6.1.4.1.9.9.122 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCasaMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is supported only on Cisco uBR7100 series and Cisco uBR7200 series routers that are running a Cisco IOS "-is-" software image.
- This MIB is not supported on the Cisco uBR10012 router.

CISCO-CDP-MIB

The CISCO-CDP-MIB contains objects to manage the Cisco Discovery Protocol (CDP) on the router, and to display the contents of the CDP neighbor table.

The MODULE-IDENTITY for the CISCO-CDP-MIB is ciscoCdpMIB, and its top-level OID is 1.3.6.1.4.1.9.9.23 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCdpMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-CIRCUIT-INTERFACE-MIB

The CISCO-CIRCUIT-INTERFACE-MIB contains objects to manage circuits on circuit-based interfaces, such as ATM or Frame Relay.

The MODULE-IDENTITY for the CISCO-CIRCUIT-INTERFACE-MIB is ciscoCircuitInterfaceMIB, and its top-level OID is 1.3.6.1.4.1.9.9.160 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCircuitInterfaceMIB).

MIB Constraints

This MIB is not supported in any Cisco IOS Release 12.1EC software image.

CISCO-CLASS-BASED-QOS-MIB

The CISCO-CLASS-BASED-QOS-MIB provides access to quality of service (QoS) configuration information and statistics. The MIB uses several indexes to identify QoS features and distinguish among instances of those features:

- cbQosPolicyIndex—Identifies a service policy attached to a logical interface.
- cbQosObjectsIndex—Identifies each QoS feature on a Cisco uBR7200 and the uBR10k routers.
- 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.

Note Do not reuse these indexes 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 run-time instance. Multiple instances of a QoS feature have a separate statistics object. Run-time instances of QoS objects are each assigned a unique identifier (cbQosObjectsIndex) to distinguish among multiple objects with matching configurations.

The MODULE-IDENTITY for the CISCO-CLASS-BASED-QOS-MIB is ciscoCBQosMIB, and its top-level OID is 1.3.6.1.4.1.9.9.166 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCBQosMIB).

MIB Constraints

Table 3-9 lists the constraints that the Cisco uBR7200 series router places on objects in the CISCO-CLASS-BASED-QOS-MIB. For detailed definitions of MIB objects, see the standard MIB file. Any MIB table or object not listed in this table is implemented as defined in the MIB.

Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints for the uBR7200 Series Router

MIB Object	Notes
cbQosFrameRelayPolicyTable	
• cbQosFRPolicyIndex	Not supported. Always 0.
• cbQosFrDLCI	Not supported. Always 0.
cbQosATMPVCPolicyTable	
• cbQosAtmVCI	Not supported. Always 0.
• cbQosATMPolicyIndex	Not supported. Always 0.
• cbQosAtmVPI	Not supported. Always 0.
cbQosQueueingCfgTable	
• cbQosQueueingCfgFlowEnabled·	Not supported. Always false(2).
• cbQosInterfacePolicyIndex	Not supported. Always 0.
• cbQosQueueingCfgIndividualQSize·	Not supported. Always 0.
• cbQosQueueingCfgDynamicQNumber·	Not supported. Always 0.
• cbQosQueueingCfgPrioBurstSize	Not supported. Always 0.
cbQosREDCfgTable	
• cbQosREDCfgMeanQsize	Not supported for PRE1. Always 0.
• cbQosREDCfgDscpPrec	DSCP-based is not supported.
cbQosREDClassCfgTable	
	If IP precedence is configured for the policy. • For PRE1, this table will have entries for all seven IP precedences. The MIB objects in cbQosREDClassCfgEntry will have a value of 0 if IP precedence is not configured for the policy. • For PRE2, this table will only have an entry for the configured IP precedence.
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	Not supported. Always 0.
• cbQosCMDropByteOverflow	Not supported. Always 0.
• cbQosCMDropByte	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.
cbQosREDCfgTable	
• cbQosREDCfgMeanQsize	Not supported for PRE1. Always 0.
• cbQosREDCfgDscpPrec	DSCP-based is not supported.
cbQosREDClassCfgTable	
	If IP precedence is configured for the policy. • For PRE1, this table will have entries for all seven IP precedences. The MIB objects in cbQosREDClassCfgEntry will have a value of 0 if IP precedence is not configured for the policy. • For PRE2, this table will only have an entry for the configured IP precedence.
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	Not supported. Always 0.
• cbQosCMDropByteOverflow	Not supported. Always 0.
• cbQosCMDropByte	Not supported. Always 0.

Table 3-9 CISCO-CLASS-BASED-QOS-MIB Constraints for the uBR7200 Series Router

MIB Object	Notes
• cbQosQueueingDiscardByteOverflow	Not supported. Always 0.
• cbQosQueueingDiscardByte	Not supported. Always 0.
cbQosTSStatsTable	
• cbQosTSStatsDelayedByteOverflow·	Not supported. Always 0.
• cbQosTSStatsDelayedByte	Not supported. Always 0.
• cbQosTSStatsDelayedByte64	Not supported. Always 0.
• cbQosTSStatsDelayedPktOverflow	Not supported. Always 0.
• cbQosTSStatsDelayedPkt·	Not supported. Always 0.
• cbQosTSStatsDelayedPkt64	Not supported. Always 0.
• cbQosTSStatsDropByteOverflow	Not supported. Always 0.
• cbQosTSStatsDropByte	Not supported. Always 0.
• cbQosTSStatsDropByte64	Not supported. Always 0.
• cbQosTSStatsActive	Not dynamic. If traffic shaping is configured, then cbQosTSStatsActive is true(1); otherwise, it is false(2).
cbQosREDClassStatsTable	
• cbQosREDRandomDropPktOverflow • cbQosREDRandomDropPkt • cbQosREDRandomDropPkt64	Counts are recorded per class, not per cbQosREDValue (IP precedence). All counters with the same cbQosPolicyIndex and cbQosObjectsIndex contain the same count.
• cbQosREDRandomDropByteOverflow • cbQosREDRandomDropByte • cbQosREDRandomDropByte64	Not supported. Always 0.
• cbQosREDTailDropPktOverflow • cbQosREDTailDropPkt • cbQosREDTailDropPkt64	Counts are recorded per class, not per cbQosREDValue (IP precedence). All counters with the same cbQosPolicyIndex and cbQosObjectsIndex contain the same count.
• cbQosREDTailDropByteOverflow • cbQosREDTailDropByte • cbQosREDTailDropByte64	Not supported. Always 0.
• cbQosREDTransmitPktOverflow • cbQosREDTransmitPkt • cbQosREDTransmitPkt64 • cbQosREDTransmitByteOverflow • cbQosREDTransmitByte • cbQosREDTransmitByte64	Counts are recorded per class, not per cbQosREDValue (IP precedence). All counters with the same cbQosPolicyIndex and cbQosObjectsIndex contain the same count.

CISCO-COMPRESSION-SERVICE-ADAPTER-MIB

The CISCO-COMPRESSION-SERVICE-ADAPTER-MIB contains objects with statistics and status information for hardware-based compression service adapters that are installed in the router.

The MODULE-IDENTITY for the CISCO-COMPRESSION-SERVICE-ADAPTER-MIB is ciscoCompressionServiceAdapterMIB, and its top-level OID is 1.3.6.1.4.1.9.9.57 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCompressionServiceAdapterMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB exists on Cisco uBR7100 series and Cisco uBR7200 series routers, but is not supported because these routers do not support any compression service adapter line cards.
- This MIB is not supported on the Cisco uBR10012 router.

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

The MODULE-IDENTITY for the CISCO-CONFIG-COPY-MIB is ciscoConfigCopyMIB, and its top-level OID is 1.3.6.1.4.1.9.9.96 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoConfigCopyMIB).

MIB Constraints

This MIB has the following constraints.

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

MIB Object	Notes
ccCopyTable	
• ccCopyProtocol	Only the Trivial File Transfer Protocol, tftp(1), is supported. The File Transfer Protocol, ftp(2), and remote copy protocol, rcp(3), are not supported.
• ccCopySourceFileType ccCopyDestFileType	The values iosFile(2) and terminal(5) are not supported for source and destination file types.
• cCopyUserName and ccCopyUserPassword	Not supported, because it is only valid when FTP and Remote Copy Protocol (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.

The MODULE-IDENTITY for the CISCO-CONFIG-MAN-MIB is ciscoConfigManMIB, and its top-level OID is 1.3.6.1.4.1.9.9.43 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoConfigManMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-DOCS-EXT-MIB

The CISCO-DOCS-EXT-MIB contains objects that support extensions to the Data-over-Cable Service Interface Specifications (DOCSIS) interface MIB, DOCS-IF-MIB. In addition, this MIB:

- Includes attributes to configure the (DMIC) dynamic shared secret feature.
- Generate traps when a cable modem fails the shared-secret security checks.
- Allows the CMTS to help ensure that every online cable modem uses the DOCSIS configuration file assigned to it.

This support protects against theft-of-service attempts from subscribers and safeguards operators against stolen or fraudulently downloaded configuration files. Configuration files are signed with a shared secret that is verified when a cable modem connects to the CMTS.

This MIB includes objects to manage the Cisco CMTS, as well as to manage the following:

- Quality of service (QoS) configuration on the router.
- DOCSIS 1.0 cable modems and customer premises equipment (CPE) devices, including counters for the number of cable modems on each interface.
- Spectrum management of the upstream channels—Objects that keep count of the total # of modems, # of registered and # of active modems on the interface as well as each upstream.
- CM CPE (customer premises equipment) information—Two new tables have been added to the CISCO-DOCS-EXT-MIBto query CPE information:
  - cdxCmToCpeTable contains objects about CPE connects behind cable modem. It provides information on IP address and IP address type of each CPE connect to a CM.
  - cdxCpeToCmTable contains objects that query information about cable modems with CPE connects.

Note This MIB provides information for DOCSIS 1.0 cable modems. For DOCSIS 1.1 cable modems, see DOCS-QOS-MIB.

The MODULE-IDENTITY for the CISCO-DOCS-EXT-MIB is ciscoDocsExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.116.1.3.7 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoDocsExtMIB). One of the most commonly used OID is ccsFlapObjects.ccsFlapTable.ccsFlapEntry.ccsFlapInsertionFails (1.3.6.1.4.1.9.9.114.1.1.5.1.4).

Wideband Support in Cisco IOS Release 12.3(23)BC

This MIB module includes objects for the scheduler that support Quality of Service (QoS) of MCNS/DOCSIS compliant Radio Frequency (RF) interfaces. Also this MIB shows various states of the schedulers enabling you to monitor of the schedulers' current status.

- RateLimit: The MC interface layer is not supported.
- Bandwidth Queue: This is only supported on the Cable interface upstream, and there is no downstream support for MC interfaces.

MIB Constraints

This MIB has the following constraints.

Table 3-11 CISCO-DOCS-EXT-MIB Constraints

MIB Object	Notes
cdxCmToCpeTable	
cdxCpeToCmTable	
cdxCmCpeTable	Using GET-NEXT requests to retrieve the rows of this table might require lengthy, time-consuming searches on the MAC address, which could consume excessive amounts of CPU processor time when the table is large. Retrieve the individual rows using a GET request that uses the device's MAC address as the table index. This avoids possible performance problems and also ensures that the retrieved rows contain the most current, real-time data for those devices.
cdxCmCpeAccessGroup	The Cisco uBR10012 router does not support the objects in cdxCmCpeAccessGroup (equivalent to the **cable host access-group** command). On the Cisco uBR10012 router, use the similar functionality in the DOCS-SUBMGT-MIB.
cdxIfUpChannelTable	
• cdxIfUpChannelNumActiveUGS cdxIfUpChannelMaxUGSLastOneHour cdxIfUpChannelMinUGSLastOneHour cdxIfUpChannelAvgUGSLastOneHour cdxIfUpChannelMaxUGSLastFiveMins cdxIfUpChannelMinUGSLastFiveMins cdxIfUpChannelAvgUGSLastFiveMins	These objects related to Unsolicited Grant Service (UGS) flows are supported only in Cisco IOS Release 12.1(8)EC, Cisco IOS Release 12.2(15)BC1a, and later releases.

Table 3-11 CISCO-DOCS-EXT-MIB Constraints (continued)

MIB Object	Notes
• cdxIfUpChannelAvgLastOneHour	Displays accurate values only in Cisco IOS Release 12.1(8)EC, Cisco IOS Release 12.2(15)BC1a, and later releases
cdxCmtsServiceExtTable	Reports the downstream traffic counters only for cable modems that are provisioned for DOCSIS 1.0 operation. For DOCSIS 1.1 and DOCSIS 2.0 cable modems, use the docsQosServiceFlowStatsTable in DOCS-QOS-MIB.
cdxCmtsCmTable	
• cdxCmtsCmQosProfile	Associating a cable modem to a QoS profile is supported only in Cisco IOS Release 12.1(19)EC and Release 12.2(11)BC2 and later releases.
• cdxCmCpeEntry	When a Cisco uBR7100 series router is running in bridging mode, it is possible for the same IP address to appear for different MAC addresses in the cdxCmCpeEntry rows. This occurs when the first device goes offline, and its IP address is given to a second device. Because the router is in bridging mode, it cannot extract the IP addresses from DHCP requests, and so assumes all IP addresses are static. This is expected behavior while in bridging mode and does not occur when the router is operating in the default behavior of routing mode. • A GET request for cdxCmCpeEntry returns NULL if the router is already processing another request for this table (either by an SNMP GET or CLI **show** command). • A null is also returned if the router is processing a request for any other table that is indexed by cable modem or CPE MAC address, such as cdrqCmtsCmStatusTable, docsIfCmtsMacToCmTable, and docsQosCmtsMacToSrvFlowTable. Wait until the first request is done and then repeat the request for cdxCmCpeEntry.
cdxCmtsCmStatusExtTable • cdxIfCmtsCmStatusLastResetTime • cdxIfCmtsCmStatusOnlineTimesNum	
cdxCmtsCmStatusDMICTable	This table contains the list of modems which failed the CMTS Dynamic Message Integrity Check (DMIC).

Table 3-11 CISCO-DOCS-EXT-MIB Constraints (continued)

MIB Object	Notes
• cdxCmtsCmDMICMode	The DMIC feature operates in the following modes, depending on what action should be taken for cable modems that fail the CMTS DMIC verification check: • notConfigured(1)—Indicates that the DMIC is not configured for this cable interface. • mark(2)—By default, the DMIC feature is enabled on all cable interfaces using the mark option. In this mode, the CMTS allows cable modems to come online even if they fail the CMTS DMIC validity check. • lock(3)—When the lock option is used, the CMTS assigns a restrictive QoS configuration to CMs that fail the DMIC validity check twice in a row. A particular QoS profile is used for locked cable modems and is specified by setting cdxCmtsCmDMICLockQos. If a customer resets their CM, the CM will reregister but still uses the restricted QoS profile. A locked CM continues with the restricted QoS profile until it goes offline and remains offline for at least 24 hours, at which point it is allowed to reregister with a valid DOCSIS configuration file. A system operator can manually clear the lock on a CM by setting the cdxCmtsCmStatusDMICUnLock object. • reject(4)—In the reject mode, the CMs cannot go online if they fail the CMTS DMIC validity check.
• cdxCmtsCmDMICLockQos	If cdxCmtsCmDMICMode is set to lockingMode(3), this object would contain the restrictive QoS profile number as indicated by docsIfQosProfIndex if set and it will have a value of zero (0) if not applicable or not defined. If, cdxCmtsCmDMICMode is set to lockingMode(3) and this object is not defined, then the CMTS defaults to special QoS profile that limits the downstream and upstream service flows to a maximum rate of 10 kbps. However, for this to happen the modems should have the permission to create QoS profile.

CISCO-DOCS-REMOTE-QUERY-MIB

The CISCO-DOCS-REMOTE-QUERY-MIB contains the objects that are monitored and collected by the remote query feature, which is enabled using the **cable modem remote-query** command on the Cisco CMTS.

The MODULE-IDENTITY for the CISCO-DOCS-REMOTE-QUERY-MIB is ciscoDocsRemoteQueryMIB, and its top-level OID is 1.3.6.1.4.1.9.10.59 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoDocsRemoteQueryMIB). One of the most commonly used OID is cdrqCmtsCmSigQSignalNoise (1.3.6.1.4.1.9.10.59.1.2.1.1.4).

MIB Constraints

This MIB has the following constraints.

- This MIB is supported only in Cisco IOS Release 12.2(4)BC1 and later releases.
- This MIB is not supported on the Cisco uBR10012 router.

Table 3-12 CISCO-DOCS-REMOTE-QUERY-MIB Constraints

MIB Object	Notes
cdrqCmtsCmStatusTable	We do not recommend using GET-NEXT requests to retrieve the rows of this table, because it could require lengthy, time-consuming searches on the MAC address, which could consume excessive amounts of CPU processor time when the table is large. Retrieve the individual rows using a GET request that uses the device's MAC address as the table index. This prevents possible performance problems and also ensures that the retrieved rows contain the most current, real-time data for those devices. A GET request for cdrqCmtsCmStatusTable returns NULL if the router is already processing another request for this table (either by an SNMP GET or CLI **show** command). A null is also returned if the router is processing a request for any other table that is indexed by CM or CPE MAC address, such as cdxCmCpeEntry, docsIfCmtsMacToCmTable, and docsQosCmtsMacToSrvFlowTable. Wait until the first request is done and then repeat the request for cdrqCmtsCmStatusTable.

CISCO-ENHANCED-MEMPOOL-MIB

The CISCO-ENHANCED-MEMPOOL-MIB contains objects to monitor the status of memory pools of all physical entities in a system, including line cards that contain their own onboard processors and memory.

The CISCO-ENHANCED-MEMPOOL-MIB enables you to monitor CPU and memory utilization for cable line cards and broadband processing engines (BPEs) on the Cisco uBR10012 routers. These would include the Cisco MC16X and Cisco MC28X series line cards.

The MODULE-IDENTITY for the CISCO-ENHANCED-MEMPOOL-MIB is ciscoEnhancedMemPoolMIB, and its top-level OID is 1.3.6.1.4.1.9.9.221 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoEnhancedMemPoolMIB).

MIB Constraints

This MIB is supported only in Cisco IOS Release 12.3(9a)BC and later releases.

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.

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

MIB Constraints

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

MIB Object	Notes
ceAlarmDescrTable	Read-only.
ceAlarmFilterProfileTable	Not implemented.
ceAlarmCutOff	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 object is automatically updated whenever a line card is removed or inserted into a slot, or when you enter a command at the CLI prompt that affects the operation of a line card.

The MODULE-IDENTITY for the CISCO-ENTITY-ASSET-MIB is ciscoEntityAssetMIB, and its top-level OID is 1.3.6.1.4.1.9.9.92 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoEntityAssetMIB).

MIB Constraint

This MIB is not supported on any Cisco CMTS platforms, although it is included in the Cisco IOS software images.

CISCO-ENTITY-EXT-MIB

The CISCO-ENTITY-EXT-MIB contains objects that supplement the entityPhysicalTable in the ENTITY-MIB (RFC 2737). These objects provide information about entries in the entityPhysicalTable that have a CPU or other type of onboard processor.

The MODULE-IDENTITY for the CISCO-ENTITY-EXT-MIB is ciscoEntityExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.195 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoEntityExtMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is only supported for the physical entities representing active and standby processors.
- The set operations of ceExtConfigRegNext and ceExtSysBootImageList are only supported on the physical entity representing the active Route Processor (RP).
- Because the ceExtSysBootImageList for the secondary RP is returned from the bootvar (To display information about the BOOT environment variable), the secondary route processor ceExtSysBootImageList is only updated from the active route processor when configuration is synced from the active router processor. Use the **write memory** command to force the sync process.

CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB contains objects that supplement the entityPhysicalTable in the ENTITY-MIB (RFC 2737). These objects provide information about the configuration and operational status of entries in the entityPhysicalTable that are field-replaceable units (FRUs).

The cefcModuleTable object is automatically updated whenever a line card is removed or inserted into a slot or when you enter a command at the CLI prompt that affects the operation of the line card.

The MODULE-IDENTITY for the CISCO-ENTITY-FRU-CONTROL-MIB is ciscoEntityFRUControlMIB, and its top-level OID is 1.3.6.1.4.1.9.9.117 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoEntityFRUControlMIB).

MIB Constraints

Table 3-14 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 3-14 CISCO-ENTITY-FRU-CONTROL-MIB Constraints

MIB Object	Notes
cefcModuleTable	
• cefcModuleAdminStatus	Supported values: • Enable(1) • Reset(3) Write is not supported.
• cefcModuleOperStatus	Supported values: • Unknown(1)—Read-only. • Ok(2)—Read-only. • Failed(7)—Read-only.
• cefcModuleResetReason	Supported values: • Unknown(1)—Read-only. • PowerUp(2)—Read-only. • ManualReset(5)—Read-only.
cefcFRUPowerSupplyGroupTable	Not supported.
cefcFRUPowerSupplyTable	Not supported.
• cefcMaxDefaultInLinePower	Not supported.
• cefcPowerStatusChange	Not supported. Use ciscoEnvMonSuppStatusChangeNotif for redundant power supply.

1. The entPhysicalEntry (which has module(9) as entPhysicalClass in the entPhysicalTable) has a corresponding entry in the cefcModuleTable.

CISCO-ENTITY-SENSOR-MIB

The CISCO-ENTITY-SENSOR-MIB contains objects that supplement the entityPhysicalTable in the ENTITY-MIB (RFC 2737). These objects provide information about the entries in the entityPhysicalTable that are sensors (such as temperature sensors).

The MODULE-IDENTITY for the CISCO-ENTITY-SENSOR-MIB is entitySensorMIB, and its top-level OID is 1.3.6.1.4.1.9.9.91 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.entitySensorMIB).

MIB Constraints

This MIB has the following constraints:

- This MIB is supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers.
- This MIB is not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router. For temperature reporting, use the CISCO-ENVMON-MIB.

CISCO-ENTITY-VENDORTYPE-OID-MIB

The CISCO-ENTITY-VENDORTYPE-OID-MIB defines the object identifiers (OIDs) assigned to components in the Cisco CMTS routers. 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 card).

Note This MIB is regularly updated with OIDs for new components in the Cisco IOS software release that introduced support for those components.

The MODULE-IDENTITY for the CISCO-ENTITY-VENDORTYPE-OID-MIB is ciscoEntityVendortypeOIDMIB, and its top-level OID is 1.3.6.1.4.1.9.12.3 (iso.org.dod.internet.private.enterprises.cisco.ciscoModules.ciscoEntityVendortypeOIDMIB).

MIB Constraints

Table 3-15 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 3-15 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Constraints

MIB Object (OID Assignment)	Notes
cevChassis	
• cevChassisUbr7246 (1.3.6.1.4.1.9.12.3.1.3.57)	Cisco uBR7246 chassis
• cevChassisUbr7223 (1.3.6.1.4.1.9.12.3.1.3.68)	Cisco uBR7223 chassis
• cevChassisUbr7246Vxr (1.3.6.1.4.1.9.12.3.1.3.134)	Cisco uBR7246VXR chassis
• cevChassisUbr10012 (1.3.6.1.4.1.9.12.3.1.3.183)	Cisco uBR10012 chassis
• cevChassisUbr7111 (1.3.6.1.4.1.9.12.3.1.3.211)	Cisco uBR7111 chassis
• cevChassisUbr7111E (1.3.6.1.4.1.9.12.3.1.3.212)	Cisco uBR7111E chassis
• cevChassisUbr7114 (1.3.6.1.4.1.9.12.3.1.3.213)	Cisco uBR7114 chassis
• cevChassisUbr7114E (1.3.6.1.4.1.9.12.3.1.3.214)	Cisco uBR7114E chassis
cevPowerSupply	
• cevPowerSupplyUbr10012AC (1.3.6.1.4.1.9.12.3.1.6.150)	UBR10012 Series AC Power Entry Module
• cevPowerSupplyUbr10012DC (1.3.6.1.4.1.9.12.3.1.6.151)	UBR10012 Series DC Power Entry Module
• 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	
• cevFanTrayUbr10012 (1.3.6.1.4.1.9.12.3.1.6.151)	UBR10012 Series Fan Assembly Module
cevModule	
cevModuleCpuType	
• cevC7200Io1fe (1.3.6.1.4.1.9.12.3.1.9.5.1)	UBR7200-I/O-FE controller for Cisco uBR7200 series
• cevC7200Io (1.3.6.1.4.1.9.12.3.1.9.5.2)	UBR7200-I/O controller for Cisco uBR7200 series

Table 3-15 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Constraints (continued)

MIB Object (OID Assignment)	Notes
• cevCpu7200Npe300 (1.3.6.1.4.1.9.12.3.1.9.5.9)	NPE-300 processor for Cisco uBR7200 series
• cevCpu7200Npe175 (1.3.6.1.4.1.9.12.3.1.9.5.14)	NPE-175 processor for Cisco uBR7200 series
• cevCpu7200Npe225 (1.3.6.1.4.1.9.12.3.1.9.5.15)	NPE-225 processor for Cisco uBR7200 series
• cevCpu7200Npe100 (1.3.6.1.4.1.9.12.3.1.9.5.26)	NPE-100 processor for Cisco uBR7200 series
• cevCpu7200Npe150 (1.3.6.1.4.1.9.12.3.1.9.5.27)	NPE-150 processor for Cisco uBR7200 series
• cevCpu7200Npe200 (1.3.6.1.4.1.9.12.3.1.9.5.28)	NPE-200 processor for Cisco uBR7200 series
• cevCpu7200Npe400 (1.3.6.1.4.1.9.12.3.1.9.5.39)	NPE-400 processor for Cisco uBR7246VXR
• cevCpu7200Npeg1 (1.3.6.1.4.1.9.12.3.1.9.5.56)	NPE-G1 processor for Cisco uBR7246VXR
• cevCpuCreRp (1.3.6.1.4.1.9.12.3.1.9.5.29)	Central Routing Engine—Route processor for the Cisco uBR10012
• cevCpuCreFp (1.3.6.1.4.1.9.12.3.1. 9.5.30)	Central Routing Engine—Forwarding processor for the Cisco uBR10012
cevModuleC7xxxType	
• cevC7xxxMc14a (1.3.6.1.4.1.9.12.3.1.9.7.1)	Cisco uBR-MC14C cable interface line card
• cevC7xxxMc16a (1.3.6.1.4.1.9.12.3.1.9.7.2)	Cisco uBR-MC16C cable interface line card
• cevC7xxxMc11 (1.3.6.1.4.1.9.12.3.1.9.7.3)	Cisco uBR-MC11-FPGA cable interface line card
• cevC7xxxMc12a (1.3.6.1.4.1.9.12.3.1.9.7.4)	Cisco uBR-MC12C cable interface line card
• cevC7xxxMc11a (1.3.6.1.4.1.9.12.3.1.9.7.5)	Cisco uBR-MC11C cable interface line card
• cevC7xxxIo1feTxIsl (1.3.6.1.4.1.9.12.3.1.9.7.6)	Fast Ethernet I/O Controller
• cevC7xxxMc28 (1.3.6.1.4.1.9.12.3.1.9.7.8)	Cisco uBR-MC28C cable interface line card
• cevC7xxxIo2FE (1.3.6.1.4.1.9.12.3.1.9.7.12)	UBR7200-I/O-2FE/E controller for Cisco uBR7200 series
cevModuleUbrType (1.3.6.1.4.1.9.12.3.1.9.27)	
• cevUbrMc16s (1.3.6.1.4.1.9.12.3.1.9.27.2)	Cisco uBR-MC16S cable interface line card
• cevUbrMc11 (1.3.6.1.4.1.9.12.3.1.9.27.3)	Cisco uBR-MC11-FPGA cable interface line card
• cevUbrMc11c (1.3.6.1.4.1.9.12.3.1.9.27.4)	Cisco uBR-MC11C cable interface line card
• cevUbrMc12c (1.3.6.1.4.1.9.12.3.1.9.27.5)	Cisco uBR-MC12C cable interface line card
• cevUbrMc14c (1.3.6.1.4.1.9.12.3.1.9.27.6)	Cisco uBR-MC14C cable interface line card
• cevUbrMc16b (1.3.6.1.4.1.9.12.3.1.9.27.8)	Cisco uBR-MC16B cable interface line card
• cevUbrMc16c (1.3.6.1.4.1.9.12.3.1.9.27.9)	Cisco uBR-MC16C cable interface line card
• cevUbrMc16e (1.3.6.1.4.1.9.12.3.1.9.27.10)	Cisco uBR-MC16E cable interface line card
• cevUbrMc28c (1.3.6.1.4.1.9.12.3.1.9.27.11)	Cisco uBR-MC28C cable interface line card
• cevUbrClk (1.3.6.1.4.1.9.12.3.1.9.27.16)	Cisco National Clock Card for the Cisco uBR7246VXR router
• cevUbrMc28cBnc (1.3.6.1.4.1.9.12.3.1.9.27.22)	Cisco uBR-MC28C-BNC cable interface line card
• cevUbrMc520sD (1.3.6.1.4.1.9.12.3.1.9.27.32)	Cisco uBR-MC5X20S-D cable interface line card
• cevUbrMc28u (1.3.6.1.4.1.9.12.3.1.9.27.34)	Cisco uBR-MC28U cable interface line card

Table 3-15 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Constraints (continued)

MIB Object (OID Assignment)	Notes
• cevCpu7200Npe300 (1.3.6.1.4.1.9.12.3.1.9.5.9)	NPE-300 processor for Cisco uBR7200 series
• cevCpu7200Npe175 (1.3.6.1.4.1.9.12.3.1.9.5.14)	NPE-175 processor for Cisco uBR7200 series
• cevCpu7200Npe225 (1.3.6.1.4.1.9.12.3.1.9.5.15)	NPE-225 processor for Cisco uBR7200 series
• cevCpu7200Npe100 (1.3.6.1.4.1.9.12.3.1.9.5.26)	NPE-100 processor for Cisco uBR7200 series
• cevCpu7200Npe150 (1.3.6.1.4.1.9.12.3.1.9.5.27)	NPE-150 processor for Cisco uBR7200 series
• cevCpu7200Npe200 (1.3.6.1.4.1.9.12.3.1.9.5.28)	NPE-200 processor for Cisco uBR7200 series
• cevCpu7200Npe400 (1.3.6.1.4.1.9.12.3.1.9.5.39)	NPE-400 processor for Cisco uBR7246VXR
• cevCpu7200Npeg1 (1.3.6.1.4.1.9.12.3.1.9.5.56)	NPE-G1 processor for Cisco uBR7246VXR
• cevCpuCreRp (1.3.6.1.4.1.9.12.3.1.9.5.29)	Central Routing Engine—Route processor for the Cisco uBR10012
• cevCpuCreFp (1.3.6.1.4.1.9.12.3.1. 9.5.30)	Central Routing Engine—Forwarding processor for the Cisco uBR10012
cevModuleC7xxxType	
• cevC7xxxMc14a (1.3.6.1.4.1.9.12.3.1.9.7.1)	Cisco uBR-MC14C cable interface line card
• cevC7xxxMc16a (1.3.6.1.4.1.9.12.3.1.9.7.2)	Cisco uBR-MC16C cable interface line card
• cevC7xxxMc11 (1.3.6.1.4.1.9.12.3.1.9.7.3)	Cisco uBR-MC11-FPGA cable interface line card
• cevC7xxxMc12a (1.3.6.1.4.1.9.12.3.1.9.7.4)	Cisco uBR-MC12C cable interface line card
• cevC7xxxMc11a (1.3.6.1.4.1.9.12.3.1.9.7.5)	Cisco uBR-MC11C cable interface line card
• cevC7xxxIo1feTxIsl (1.3.6.1.4.1.9.12.3.1.9.7.6)	Fast Ethernet I/O Controller
• cevC7xxxMc28 (1.3.6.1.4.1.9.12.3.1.9.7.8)	Cisco uBR-MC28C cable interface line card
• cevC7xxxIo2FE (1.3.6.1.4.1.9.12.3.1.9.7.12)	UBR7200-I/O-2FE/E controller for Cisco uBR7200 series
cevModuleUbrType (1.3.6.1.4.1.9.12.3.1.9.27)	
• cevUbrMc16s (1.3.6.1.4.1.9.12.3.1.9.27.2)	Cisco uBR-MC16S cable interface line card
• cevUbrMc11 (1.3.6.1.4.1.9.12.3.1.9.27.3)	Cisco uBR-MC11-FPGA cable interface line card
• cevUbrMc11c (1.3.6.1.4.1.9.12.3.1.9.27.4)	Cisco uBR-MC11C cable interface line card
• cevUbrMc12c (1.3.6.1.4.1.9.12.3.1.9.27.5)	Cisco uBR-MC12C cable interface line card
• cevUbrMc14c (1.3.6.1.4.1.9.12.3.1.9.27.6)	Cisco uBR-MC14C cable interface line card
• cevUbrMc16b (1.3.6.1.4.1.9.12.3.1.9.27.8)	Cisco uBR-MC16B cable interface line card
• cevUbrMc16c (1.3.6.1.4.1.9.12.3.1.9.27.9)	Cisco uBR-MC16C cable interface line card
• cevUbrMc16e (1.3.6.1.4.1.9.12.3.1.9.27.10)	Cisco uBR-MC16E cable interface line card
• cevUbrMc28c (1.3.6.1.4.1.9.12.3.1.9.27.11)	Cisco uBR-MC28C cable interface line card
• cevUbrClk (1.3.6.1.4.1.9.12.3.1.9.27.16)	Cisco National Clock Card for the Cisco uBR7246VXR router
• cevUbrMc28cBnc (1.3.6.1.4.1.9.12.3.1.9.27.22)	Cisco uBR-MC28C-BNC cable interface line card
• cevUbrMc520sD (1.3.6.1.4.1.9.12.3.1.9.27.32)	Cisco uBR-MC5X20S-D cable interface line card
• cevUbrMc28u (1.3.6.1.4.1.9.12.3.1.9.27.34)	Cisco uBR-MC28U cable interface line card

Table 3-15 CISCO-ENTITY-VENDORTYPE-OID-MIB Objects and Constraints (continued)

MIB Object (OID Assignment)	Notes
• cevUbrMc16u (1.3.6.1.4.1.9.12.3.1.9.27.35)	Cisco uBR-MC16U cable interface line card
• cevUbrMc28ux (1.3.6.1.4.1.9.12.3.1.9.27.36)	Cisco uBR-MC28X cable interface line card
• cevUbrMc16ux (1.3.6.1.4.1.9.12.3.1.9.27.37)	Cisco uBR-MC16X cable interface line card
• cevUbrMc520uD (1.3.6.1.4.1.9.12.3.1.9.27.38)	Cisco uBR-MC5X20U-D cable interface line card
cevModule100012Type	
• cevPos1oc12 (1.3.6.1.4.1.9.12.3.1.9.32.1)	Cisco uBR10-1OC12/P-SMI OC-12 POS uplink line card
• cevGe (1.3.6.1.4.1.9.12.3.1.9.32.3)	Cisco uBR10-1GE Gigabit Ethernet uplink line card
• cevSrpOc48SmSr (1.3.6.1.4.1.9.12.3.1.9.32.11)	Cisco uBR10012 OC-48 DPT/POS interface module (short reach)
• cevSrpOc48SmLr1 (1.3.6.1.4.1.9.12.3.1.9.32.26)	Cisco uBR10012 OC-48 DPT/POS interface module (long reach)
• cevC10K48MbFlashCard (1.3.6.1.4.1.9.12.3.1.9.32.18)	48MB flash card
• cevC10K128MbFlashCard (1.3.6.1.4.1.9.12.3.1.9.32.19)	128MB flash card
• cevSpa24xWbdSfp(1.3.6.1.4.1.9.12.3.1.9.2.145)	Cisco SPA-24-XWBD-SFP shared port adapter (cevPortGe)

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. In Cisco IOS Release 12.2BC and later releases, use this MIB instead of CISCO-ENTITY-SENSOR-MIB for temperature monitoring.

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).

The MODULE-IDENTITY for the CISCO-ENVMON-MIB is ciscoEnvMonMIB, and its top-level OID is 1.3.6.1.4.1.9.9.13 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoEnvMonMIB).

MIB Constraints

Table 3-16 lists the constraints that the router places on objects in the CISCO-ENVMON-MIB.

This MIB is supported for:

- Cisco uBR7100 series and Cisco uBR7200 series routers only in Cisco IOS Release 12.1(11)EC and Cisco IOS Release 12.2(4)BC1 and later releases.
- Cisco uBR10012 routers only in Cisco IOS Release 12.2(8)BC2 and later releases.

For detailed definitions of MIB objects, see the MIB.

Table 3-16 CISCO-ENVMON-MIB Constraints

MIB Object	Notes
ciscoEnvMonTable	
• ciscoEnvMonEnableStatChangeNotif	Supported in IOS Release 12.3(18)BC and later releases. This variable indicates whether the system produces the ciscoEnvMonVoltStatusChangeNotif, ciscoEnvMonTempStatusChangeNotif, ciscoEnvMonFanStatusChangeNotif and ciscoEnvMonSuppStatusChangeNotif. A false value will prevent these notifications from being generated by the uBR system.
• ciscoEnvMonEnableVoltageNotification	Notification had been deprecated. Use ciscoEnvMonEnableStatChangeNotif.
• ciscoEnvMonEnableTemperatureNotification	
• ciscoEnvMonEnableFanNotification,	
• ciscoEnvMonEnableRedundantSupply	
ciscoEnvMonTemperatureStatusTable	
• ciscoEnvMonEnableTemperatureNotification • ciscoEnvMonTemperatureNotification	Supported values are: • ubr7200(8) for the Cisco uBR7100 series and Cisco uBR7200 series routers • c10000(10) for the Cisco uBR10012 router.
ciscoEnvMonVoltageStatusTable	
• ciscoEnvMonVoltageNotification	Not supported for the Cisco uBR10012 router.
• ciscoEnvMonEnableVoltageNotification	Supported in Cisco IOS Release 12.1(19)EC, Cisco IOS Release 12.2(4)BC, and later releases.
ciscoEnvMonFanStatusTable	• Not supported for Cisco uBR7100 series and Cisco uBR7200 series routers. • Supported for the Cisco uBR10012 router only in Cisco IOS Release 12.2(11)BC1 and later releases.
• ciscoEnvMonFanStatusIndex	Always 1. Only one table row supported for fan tray.
• ciscoEnvMonFanStatusDescr	Always Fan Tray.
• ciscoEnvMonFanState	Supported values are: • normal(1)—Both fans are working • warning(2)—One fan is failing • critical(3)—Both fans are failing • notPresent(5)—Fan tray is missing • notFunctioning(6)—Unable to get status

Table 3-16 CISCO-ENVMON-MIB Constraints

MIB Object	Notes
ciscoEnvMonSupplyStatusTable	• Supported in Cisco IOS Release 12.1 EC and in Cisco IOS Release 12.2(11)BC1 and later releases. • On the Cisco uBR7200 series routers, this table reports accurate results only in Cisco IOS Release 12.1(19)EC, Cisco IOS Release 12.2(15)BC1, and later releases.
• ciscoEnvMonSupplyStatusIndex	For uBR10012: • 1 indicates PEM0 • 2 indicates PEM1
• ciscoEnvMonSupplyStatusDescr	For uBR10012 valid values are PEM0 or PEM1.
• ciscoEnvMonSupplyState	Supported values are the following: • normal(1)—Power supply is working • critical(3)—Power supply is failing • notPresent(5)—Power supply is missing
• ciscoEnvMonSupplySource	Supported values are: • unknown(1)—Missing or unknown power supply • ac(2)—AC power supply • dc(3)—DC power supply
ciscoEnvMonAlarmContacts	Not implemented.

CISCO-FLASH-MIB

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

The MODULE-IDENTITY for the CISCO-FLASH-MIB is ciscoFlashMIB, and its top-level OID is 1.3.6.1.4.1.9.9.10 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoFlashMIB).

MIB Constraints

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 MODULE-IDENTITY for the CISCO-FRAME-RELAY-MIB is ciscoFrameRelayMIB, and its top-level OID is 1.3.6.1.4.1.9.9.49 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoFrameRelayMIB).

MIB Constraints

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.

The MODULE-IDENTITY for the CISCO-FTP-CLIENT-MIB is ciscoFtpClientMIB, and its top-level OID is 1.3.6.1.4.1.9.9.80 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoFtpClientMIB).

MIB Constraints

This MIB is not supported on any Cisco CMTS platforms, although it is included in the Cisco IOS software images.

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 Hot Standby Router Protocol (HSRP) IP addresses, monitoring the operational status of interfaces, and modifying an HSRP group's priority.

The MODULE-IDENTITY for the CISCO-HSRP-EXT-MIB is ciscoHsrpExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.107 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoHsrpExtMIB).

MIB Constraints

This MIB is not supported on any Cisco CMTS platforms, although it is included in the Cisco IOS software images.

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.

The MODULE-IDENTITY for the CISCO-HSRP-MIB is ciscoHsrpMIB, and its top-level OID is 1.3.6.1.4.1.9.9.106 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoHsrpMIB).

MIB Constraint

This MIB is not supported on any Cisco CMTS platforms, although it is included in the Cisco IOS software images.

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 draft, *Definitions of Supplemental Managed Objects for ATM Interface*, Section 9, "ATM Related Trap Support," which is available at the following URL:

http://www4.ietf.org/proceedings/03jul/I-D/draft-ietf-atommib-atm2-19.txt

The MODULE-IDENTITY for the CISCO-IETF-ATM2-PVCTRAP-MIB is ciscoIetfAtm2PvctrapMIB, and its top-level OID is 1.3.6.1.4.1.9.10.29 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIetfAtm2PvctrapMIB).

MIB Constraint

This MIB is not supported on any Cisco CMTS platforms, although it is included in the Cisco IOS software images.

CISCO-IETF-IP-FORWARD-MIB

The CISCO-IETF-IP-FORWARD-MIB contains objects that manage and describe the forwarding of IP traffic across networks that might use different versions of IP (IPv4 and IPv6).

This MIB was derived from the initial version of the Internet Draft that is being drafted to replace the current IP-FORWARD-MIB, which is defined in RFC 2096, *IP Forwarding Table MIB*. Cisco implemented this temporary MIB to provide this functionality until the Internet Draft is finalized and a new RFC is released to replace RFC 2096.

The MODULE-IDENTITY for the CISCO-IETF-IP-FORWARD-MIB is ciscoIetfIpForward, and its top-level OID is 1.3.6.1.4.1.9.10.85 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIetfIpForward).

MIB Constraints

This MIB is not supported on:

- Cisco uBR10012 router.
- Any Cisco IOS Release 12.1EC software image.

CISCO-IETF-IP-MIB

The CISCO-IETF-IP-MIB contains objects to manage the IP and ICMP protocols across networks that might use different versions of IP (IPv4 and IPv6).

This MIB was derived from the initial version of the Internet Draft that is being drafted to replace the current IP-MIB, which is defined in RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*. Cisco implemented this temporary MIB to provide this functionality until the Internet Draft is finalized and a new RFC is released to replace RFC 2011.

The MODULE-IDENTITY for the CISCO-IETF-IP-MIB is ciscoIetfIpMIB, and its top-level OID is 1.3.6.1.4.1.9.10.86 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIetfIpMIB).

MIB Constraints

This MIB is not supported on:

- Any Cisco IOS Release 12.1EC software image.
- Cisco uBR10012 router.

CISCO-IETF-NAT-MIB

The CISCO-IETF-NAT-MIB contains objects about the operation of Network Address Translation (NAT) on the router, as defined in RFC 3022. This includes objects about NAT configuration, NAT bindings, and run-time statistics.

This MIB was derived from the initial version of the Internet Draft that is being drafted to provide this support. Cisco implemented this temporary MIB to provide this functionality until the Internet Draft is finalized and a new RFC is released.

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

MIB Constraints

This MIB is:

- Supported only on Cisco uBR7100 series and Cisco uBR7200 series routers that are running a Cisco IOS Release 12.2BC “-is-” software image.
- Not supported on any Cisco IOS Release 12.1EC software image.
- Not supported on the Cisco uBR10012 router.

CISCO-IMAGE-MIB

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

The MODULE-IDENTITY for the CISCO-IMAGE-MIB is ciscoImageMIB, and its top-level OID is 1.3.6.1.4.1.9.9.25 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoImageMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-IP-ENCRYPTION-MIB

The CISCO-IP-ENCRYPTION-MIB contains objects that provide information about encrypted IP traffic on the router and the crypto maps that are being used.

The MODULE-IDENTITY for the CISCO-IP-ENCRYPTION-MIB is ciscoIpEncryptionMIB, and its top-level OID is 1.3.6.1.4.1.9.9.52 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIpEncryptionMIB).

MIB Constraints

This MIB is:

- Supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router.

CISCO-IPMROUTE-MIB

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

The MODULE-IDENTITY for the CISCO-IPMROUTE-MIB is ciscoIpMRouteMIB, and its top-level OID is 1.3.6.1.4.1.9.10.2 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIpMRouteMIB).

MIB Constraints

There are no constraints on this MIB.

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.

The MODULE-IDENTITY for the CISCO-IP-STAT-MIB is ciscoIpStatMIB, and its top-level OID is 1.3.6.1.4.1.9.9.84 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIpStatMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-IPSEC-FLOW-MONITOR-MIB

The CISCO-IPSEC-FLOW-MONITOR-MIB contains objects to manage IPSec-based virtual private networks (VPNs). These objects include information about Internet Key Exchange (IKE) negotiations and tunnels, data tunnels, historical trending analysis, and packet counters. This MIB also defines notifications about possible failures and intrusion attempts on the network.

The MODULE-IDENTITY for the CISCO-IPSEC-FLOW-MONITOR-MIB is ciscoIpSecFlowMonitorMIB, and its top-level OID is 1.3.6.1.4.1.9.9.171 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIpSecFlowMonitorMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-IPSEC-MIB

The CISCO-IPSEC-MIB contains objects about features that are used to configure and manage IPSec-based virtual private networks (VPNs).

The MODULE-IDENTITY for the CISCO-IPSEC-MIB is ciscoIPsecMIB, and its top-level OID is 1.3.6.1.4.1.9.10.62 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoIPsecMIB).

MIB Constraint

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

CISCO-IPSEC-POLICY-MAP-MIB

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

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

MIB Constraint

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

CISCO-ISDN-MIB

The CISCO-ISDN-MIB contains objects that describe the status of ISDN interfaces on the router.

The MODULE-IDENTITY for the CISCO-ISDN-MIB is ciscoIsdnMib, and its top-level OID is 1.3.6.1.4.1.9.9.26 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoIsdnMib).

MIB Constraint

This MIB is not supported on the Cisco uBR10012 router.

CISCO-LEC-DATA-VCC-MIB

The CISCO-LEC-DATA-VCC-MIB is a Cisco extension to the standard ATM-MIB. This MIB contains objects that identify the VCCs that carry packets being sent on LAN Emulation (LANE) VLANs over ATM interfaces.

The MODULE-IDENTITY for the CISCO-LEC-DATA-VCC-MIB is ciscoLecDataVccMIB, and its top-level OID is 1.3.6.1.4.1.9.9.69 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoLecDataVccMIB).

MIB Constraints

This MIB is:

- Supported only on Cisco uBR7100 series and Cisco uBR7200 series routers running a Cisco IOS "-is-" software image.
- Not supported on the Cisco uBR10012 router.

CISCO-LEC-EXT-MIB

The CISCO-LEC-EXT-MIB is a Cisco extension to the standard ATM-MIB. This MIB contains objects that map a LAN emulation client (LEC) to its VLAN.

The MODULE-IDENTITY for the CISCO-LEC-EXT-MIB is ciscoLecExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.77 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoLecExtMIB).

MIB Constraints

This MIB is:

- Supported only on Cisco uBR7100 series and Cisco uBR7200 series routers running a Cisco IOS "-is-" software image.
- Not supported on the Cisco uBR10012 router.

CISCO-LECS-MIB

The CISCO-LECS-MIB is a Cisco extension to the standard ATM-MIB. This MIB contains objects about the configuration of LANE VLANs on the Cisco router.

The MODULE-IDENTITY for the CISCO-LECS-MIB is ciscoLecsMIB, and its top-level OID is 1.3.6.1.4.1.9.9.38 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoLecsMIB).

MIB Constraints

This MIB is:

- Supported only on Cisco uBR7100 series and Cisco uBR7200 series routers running a Cisco IOS "-is-" software image.
- Not supported on the Cisco uBR10012 router.

CISCO-LES-MIB

The CISCO-LES-MIB is a Cisco extension to the standard ATM-MIB. This MIB contains objects to manage LAN emulation services (LES) on the router.

The MODULE-IDENTITY for the CISCO-LES-MIB is ciscoLesMIB, and its top-level OID is 1.3.6.1.4.1.9.9.39 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoLesMIB).

MIB Constraints

This MIB is:

- Supported only on Cisco uBR7100 series and Cisco uBR7200 series routers running a Cisco IOS "-is-" software image.
- Not supported on the Cisco uBR10012 router.

CISCO-MEMORY-POOL-MIB

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

The MODULE-IDENTITY for the CISCO-MEMORY-POOL-MIB is ciscoMemoryPoolMIB, and its top-level OID is 1.3.6.1.4.1.9.9.48 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoMemoryPoolMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-NBAR-PROTOCOL-DISCOVERY-MIB

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

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

MIB Constraints

This MIB is supported:

- Only on Cisco uBR7246VXR universal broadband routers.
- In Cisco IOS Release 12.2(15)BC2 and later releases.
- Not supported in Cisco IOS Release 12.1 EC.

CISCO-NDE-MIB

The CISCO-NDE-MIB contains objects about the configuration and operation of the Netflow Data Export (NDE) feature.

The MODULE-IDENTITY for the CISCO-NDE-MIB is ciscoNDEMIB, and its top-level OID is 1.3.6.1.4.1.9.9.226 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoNDEMIB).

MIB Constraints

This MIB is:

- Supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router.

CISCO-NTP-MIB

The CISCO-NTP-MIB contains objects to monitor the Network Time Protocol (NTP) clients and servers that are operating on the router.

The MODULE-IDENTITY for the CISCO-NTP-MIB is ciscoNtpMIB, and its top-level OID is 1.3.6.1.4.1.9.9.168 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoNtpMIB).

MIB Constraints

This MIB is:

- Supported only in Cisco IOS Release 12.2BC for the Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router.

CISCO-PIM-MIB

The CISCO-PIM-MIB defines 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.

The MODULE-IDENTITY for the CISCO-PIM-MIB is ciscoPimMIB, and its top-level OID is 1.3.6.1.4.1.9.9.184 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoPimMIB).

MIB Constraints

This MIB is supported only in Cisco IOS Release 12.2BC software images. It is not supported in Cisco IOS Release 12.1EC software images.

CISCO-PING-MIB

The CISCO-PING-MIB contains objects to manage ICMP echo (ping) requests on the router.

The MODULE-IDENTITY for the CISCO-PING-MIB is ciscoPingMIB, and its top-level OID is 1.3.6.1.4.1.9.9.16 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoPingMIB).

MIB Constraints

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.

The MODULE-IDENTITY for the CISCO-PPPOE-MIB is ciscoPppoeMIB, and its top-level OID is 1.3.6.1.4.1.9.9.194 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoPppoeMIB).

MIB Constraints

This MIB is not supported:

- On the Cisco uBR10012 router.
- In any Cisco IOS Release 12.1EC software image.

CISCO-PROCESS-MIB

The CISCO-PROCESS-MIB displays memory and CPU usage on the router and describes active system processes. The CISCO-PROCESS-MIB enables you to monitor CPU and memory utilization for line cards, cable interface line cards, and broadband processing engines on the Cisco uBR10012 or Cisco uBR7246VXR routers.

The MODULE-IDENTITY for the CISCO-PROCESS-MIB is ciscoProcessMIB, and its top-level OID is 1.3.6.1.4.1.9.9.109 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoProcessMIB).

MIB Constraints

This MIB supports:

- PRE2 modules on the Cisco uBR10012 routers with Cisco IOS Release 12.3(9a)BC and later BC releases.
- The Cisco uBR7246VXR router and the Cisco uBR10012 router with the PRE1 module in Cisco IOS Release 12.2(15)BC2 and later BC releases.
- CPU statistics for processors are distributed line cards (such as the Broadband Processing Engines) are supported in Cisco IOS Release 12.3(9a)BC and later releases.

Table 3-18 lists CISCO-PROCESS-MIB constraints.:

Table 3-17 Cisco CMTS Router CISCO-PROCESS-MIB

Object Name	Description
cpmCPUTotalTable	Maintained only for the active Performance Routing Engine (PRE) on the Cisco uBR10012 router. 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.

The MODULE-IDENTITY for the CISCO-PRODUCTS-MIB is ciscoProductsMIB, and its top-level OID is 1.3.6.1.4.1.9.12.2 (iso.org.dod.internet.private.enterprises.cisco.ciscoModules.ciscoProductsMIB).

MIB Constraints

Table 3-18 lists the relevant OIDs for the Cisco CMTS routers.

Table 3-18 Cisco CMTS Router OIDs from CISCO-PRODUCTS-MIB

Object Name	Object Identifier	Description
ciscoUBR7246	1.3.6.1.4.1.9.1.179	Cisco uBR7246 universal broadband router
ciscoUBR7223	1.3.6.1.4.1.9.1.210	Cisco uBR7223 universal broadband router
ciscoUBR7246VXR	1.3.6.1.4.1.9.1.271	Cisco uBR7246VXR universal broadband router
ciscoUBR10012	1.3.6.1.4.1.9.1.317	Cisco uBR10012 universal broadband router
ciscoUBR7111	1.3.6.1.4.1.9.1.344	Cisco uBR7111 universal broadband router
ciscoUBR7111E	1.3.6.1.4.1.9.1.345	Cisco uBR7111E universal broadband router

Table 3-18 Cisco CMTS Router OIDs from CISCO-PRODUCTS-MIB (continued)

Object Name	Object Identifier	Description
ciscoUBR7114	1.3.6.1.4.1.9.1.346	Cisco uBR7114 universal broadband router
ciscoUBR7114E	1.3.6.1.4.1.9.1.347	Cisco uBR7114E universal broadband router

CISCO-QUEUE-MIB

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

The MODULE-IDENTITY for the CISCO-QUEUE-MIB is ciscoQueueMIB, and its top-level OID is 1.3.6.1.4.1.9.9.37 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoQueueMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-RMON-SAMPLING-MIB

The CISCO-RMON-SAMPLING-MIB contains objects that supplement the RMON-MIB and the RMON2-MIB, providing additional information about the statistical reliability of the estimated counter values in these MIBs.

The MODULE-IDENTITY for the CISCO-RMON-SAMPLING-MIB is ciscoRmonSamplingMIB, and its top-level OID is 1.3.6.1.4.1.9.9.104 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoRmonSamplingMIB).

MIB Constraints

There are no constraints on this MIB.

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 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.

The MODULE-IDENTITY for the CISCO-RTTMON-MIB is ciscoRttMonMIB, and its top-level OID is 1.3.6.1.4.1.9.9.42 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoRttMonMIB).

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.

CISCO-SLB-EXT-MIB

The CISCO-SLB-EXT-MIB contains objects to supplement the CISCO-SLB-MIB, which provide additional information about server load balancing (SLB) operations on the router. In particular, the MIB contains objects about the Dynamic Feedback Protocol (DFP) manager and Layer 7 policy load balancing features.

The MODULE-IDENTITY for the CISCO-SLB-EXT-MIB is ciscoSlbExtMIB, and its top-level OID is 1.3.6.1.4.1.9.9.254 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSlbExtMIB).

MIB Constraints

This MIB is:

- Supported only in Cisco IOS Release 12.1EC "-is-" software images for the Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router.

CISCO-SLB-MIB

The CISCO-SLB-MIB contains objects about the operation of server load balancing (SLB) and the Dynamic Feedback Protocol (DFP) on the router.

The MODULE-IDENTITY for the CISCO-SLB-MIB is ciscoSlbMIB, and its top-level OID is 1.3.6.1.4.1.9.9.161 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSlbMIB).

MIB Constraints

This MIB is:

- Supported only in Cisco IOS Release 12.1EC "-is-" software images for the Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported in Cisco IOS Release 12.2BC for any Cisco CMTS router.

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.

The MODULE-IDENTITY for the CISCO-SNAPSHOT-MIB is ciscoSnapshotMIB, and its top-level OID is 1.3.6.1.4.1.9.9.19 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSnapshotMIB).

MIB Constraints

There are no constraints on this MIB.

CISCO-SRP-MIB

The CISCO-SRP-MIB contains objects to monitor and configure Spatial Reuse Protocol (SRP) interfaces and rings.

The MODULE-IDENTITY for the CISCO-SRP-MIB is ciscosrpMIB, and its top-level OID is 1.3.6.1.4.1.9.10.60 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscosrpMIB).

MIB Constraints

This MIB is not supported on Cisco uBR7100 series and Cisco uBR7200 series routers.

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 Simple Network Management Protocol (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.

The MODULE-IDENTITY for the CISCO-SYSLOG-MIB is ciscoSyslogMIB, and its top-level OID is 1.3.6.1.4.1.9.9.41 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSyslogMIB).

MIB Constraints

This MIB does not track messages generated by **debug** commands that are entered through the CLI.

Note When you plan to enable traps for SYSLOG events, increase the trap queue size from its default of 10, using the **snmp-server queue-length** command. The size of the queue can range from 1 to 1000 traps, and we recommend a size of at least 100 for systems that are sending traps for SYSLOG events.

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 TCP-MIB.

The MODULE-IDENTITY for the CISCO-TCP-MIB is ciscoTcpMIB, and its top-level OID is 1.3.6.1.4.1.9.9.6 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoTcpMIB).

MIB Constraint

This MIB is not supported on Cisco CMTS platforms, even though it is included in the Cisco IOS software images.

CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

The CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB maps the Virtual Local Area Network (VLAN) group ID to the interface index for routed VLAN interfaces.

The MODULE-IDENTITY for the CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB is ciscoVlanIfTableRelationshipMIB, and its top-level OID is 1.3.6.1.4.1.9.9.128 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoVlanIfTableRelationshipMIB).

MIB Constraint

This MIB is not supported on Cisco CMTS platforms, even though it is included in the Cisco IOS software images.

CISCO-VPDN-MGMT-EXT-MIB

The CISCO-VPDN-MGMT-EXT-MIB supplements the CISCO-VPDN-MGMT-MIB with additional information about virtual private dial-up network (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.

The MODULE-IDENTITY for the CISCO-VPDN-MGMT-EXT-MIB is ciscoVpdnMgmtExtMIB, and its top-level OID is 1.3.6.1.4.1.9.10.51 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoVpdnMgmtExtMIB).

MIB Constraints

This MIB is:

- Read-only, which means that you cannot use the MIB to configure VPDN on the router.
- Supported only on Cisco IOS “-is-” software images for Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported on the Cisco uBR10012 router.

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 3-19 for information about template name restrictions and and their effect on SNMP.

The MODULE-IDENTITY for the CISCO-VPDN-MGMT-MIB is ciscoVpdnMgmtMIB, and its top-level OID is 1.3.6.1.4.1.9.10.24 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.ciscoVpdnMgmtMIB).

MIB Constraints

This MIB is:

- Read-only, which means that you cannot use the MIB to configure VPDN on the router.
- Supported only on Cisco IOS Release 12.2BC "-is-" software images for Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported on the Cisco uBR10012 router.

The MIB objects in Table 3-19 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 3-19 Deprecated CISCO-VPDN-MGMT-MIB Objects

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, then in order to retrieve any table entries, you must use individual GET requests to retrieve each template name (cvpdnTemplateName) that does not exceed 128 characters.

CISCO-VSIMASTER-MIB

The CISCO-VSIMASTER-MIB contains objects about the master side of the the Virtual Switch Interface (VSI) protocol that is used to control ATM interfaces.

The MODULE-IDENTITY for the CISCO-VSIMASTER-MIB is ciscoVsiMasterMIB, and its top-level OID is 1.3.6.1.4.1.9.9.162 (iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoVsiMasterMIB).

MIB Constraints

This MIB is:

- Supported only on Cisco IOS Release 12.2BC software images. It is not supported on Cisco IOS Release 12.1EC software images.
- Not supported on the Cisco uBR10012 router.

DOCS-BPI-MIB

The DOCS-BPI-MIB contains objects to configure, operate, and monitor the DOCSIS 1.0 Baseline Privacy Interface (BPI) feature. This MIB has been released as RFC 3083, *Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems*.

The MODULE-IDENTITY for the DOCS-BPI-MIB is docsBpiMIB, and its top-level OID is 1.3.6.1.2.1.10.127.5 (iso.org.dod.internet.mgmt-mib-2.transmission.docsIfMIB.docsBpiMIB).

MIB Constraints

This MIB is supported only in:

- Cisco IOS software images that support DES encryption (-k8- or -k9-).
- DOCSIS 1.0 software images (Cisco IOS Release 12.1EC). In DOCSIS 1.1 software images (Cisco IOS Release 12.2BC and later releases), use the DOCS-BPI-PLUS-MIB instead.

DOCS-BPI-PLUS-MIB

The DOCS-BPI-PLUS-MIB contains objects to configure, operate, and monitor the DOCSIS 1.1 Baseline Privacy Interface Plus (BPI+) feature. This MIB is currently being reviewed as an Internet Draft, *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*. The current version is draft-ietf-ipcdn-bpiplus-mib-11.txt and is a work in progress that is subject to change without notice.

The MODULE-IDENTITY for the DOCS-BPI-PLUS-MIB is docsBpi2MIB, and its top-level OID is 1.3.6.1.2.1.10.127.6 (iso.org.dod.internet.mgmt-mib-2.transmission.docsIfMIB.docsBpi2MIB).

MIB Constraints

This MIB is supported only in:

- Cisco IOS software images that support DES encryption (-k8- or -k9-).
- DOCSIS 1.1 and DOCSIS 2.0 software images (Cisco IOS Release 12.2BC and later). In DOCSIS 1.0 software images (Cisco IOS Release 12.1EC), use the DOCS-BPI-MIB instead.
- DOCSIS BPI+ in narrowband fiber node interface configurations are supported only in Cisco IOS Release 12.3(23)BC or later on the Cisco uBR10012 router. This application of narrowband fiber nodes is distinct from additional narrowband functions supported for the Shared Port Adapter (SPA).

Table 3-20 DOCS-BPI-PLUS-MIB Constraints

MIB Object	Notes
docsBpi2CmtsCACertTable	This table cannot be used to load a root Certificate Authority (CA) certificate into the Cisco CMTS router. The root CA certificate must always be loaded on the local bootflash or Flash Disk. (For security and operational reasons, we recommend always loading the root CA certificate on the bootflash, and not on a removable Flash Disk.
docsBpi2CmtsIpMulticastMapTable **docsBpi2CmtsMulticastAuthTable.**	These tables are supported in the DOCS-BPI-PLUS-MIB in Cisco IOS Release 12.3(23)BC or later on the Cisco uBR10012 router.

DOCS-CABLE-DEVICE-MIB

The DOCS-CABLE-DEVICE-MIB contains objects to configure and monitor DOCSIS-compliant CMTS platforms and cable modem devices. This MIB was released as RFC 2669.

The MODULE-IDENTITY for the DOCS-CABLE-DEVICE-MIB is docsDev, and its top-level OID is 1.3.6.1.2.1.69 (iso.org.dod.internet.mgmt-mib-2.docsDev).

MIB Constraints

This MIB has the following constraints.

Table 3-21 DOCS-CABLE-DEVICE-MIB Constraints

MIB Object	Notes
docsDevEventTable	This table is supported in Cisco IOS Release 12.1(5)EC and later releases, and holds a maximum number of 50 events. When the table is full and a new event occurs, the oldest event is removed and replaced by the new event. The docsDevEvIndex, however, continues incrementing, up to its maximum value of 2,147,483,647.
• docsDevSerialNumber docsDevRole docsDevSTPControl	Not supported on the CMTS
• docsDevSoftware	This group of objects is not supported on the CMTS.
• docsDevCpeIpMax	Initial DOCSIS 1.1 specifications set this object to 1, but CableLabs has determined that this default can prevent PCs from communicating in certain situations (such as when the PC is booted up and defaults to a private IP address before being connected to the cable modem or before the cable modem is turned on). The cable modem must be rebooted to allow the PC to communicate. A change notice has been introduced to change the default to –1, which disables IP filtering, but this change notice has not been given final approval or been implemented. We therefore recommend configuring this parameter either to –1 or to a value greater than 1.

DOCS-CABLE-DEVICE-TRAP-MIB

The DOCS-CABLE-DEVICE-TRAP-MIB contains objects that supplement the DOCS-CABLE-DEVICE-MIB to define and configure traps and notifications for DOCSIS-compliant CMTS platforms and cable modems.

The MODULE-IDENTITY for the DOCS-CABLE-DEVICE-TRAP-MIB is docsDevTrapMIB, and its top-level OID is 1.3.6.1.2.1.69.10 (iso.org.dod.internet.mgmt-mib-2.docsDev.docsDevTrapMIB).

MIB Constraints

This MIB has the following constraints:

Table 3-22 DOCS-CABLE-DEVICE-TRAP-MIB Constraints

MIB Object	Notes
docsDevTable	
• docsIfDocsisCapability • docsIfDocsisOperMode	Both objects are deprecated.

DOCS-IF-EXT-MIB

The DOCS-IF-EXT-MIB contains objects that supplement the DOCS-IF-MIB to provide information about the capabilities and status of online cable modems.

The MODULE-IDENTITY for the DOCS-IF-EXT-MIB is docsIfExtMib, and its top-level OID is 1.3.6.1.2.1.10.127.21 (iso.org.dod.internet.mgmt.mib-2.transmission.docsIfMIB.docsIfExtMib).

MIB Constraints

Table 3-23 DOCS-IF-EXT-TRAP-MIB Constraints

MIB Object	Notes
docsDevTable	In Cisco IOS Release 12.2(15)BC1 and later releases, this MIB has been deprecated and removed as part of the support for the DOCSIS 2.0 specifications. The objects in this MIB have been replaced by new objects in the DOCS-IF-MIB and the proposed DOCS-RFI-MIB, so as to conform to the requirements given in the *DOCSIS 2.0 Operations Support System Interface Specification* (SP-OSSIv2.0-I04-030730).
• docsIfDocsisBaseCapability	Replaces docsIfDocsisCapability and docsIfDocsisOperMode
• docsIfCmtsCmStatusDocsisRegMode	Replaces docsIfCmtsCmStatusDocsisMode

DOCS-IF-MIB

The DOCS-IF-MIB contains objects to configure and monitor the radio frequency (RF) interfaces on DOCSIS-compliant CMTS platforms and cable modems. This MIB was released as RFC 2670. This MIB has been updated to draft-ietf-ipcdn-rfmibv2-05.txt.

The MODULE-IDENTITY for the DOCS-IF-MIB is docsIfMIB, and its top-level OID is 1.3.6.1.2.1.10.127 (iso.org.dod.internet.mgmt.mib-2.transmission.docsIfMIB). One of the most commonly used OIDs is docsIfUpChannelWidth (1.3.6.1.2.1.10.127.1.1.2.1.3).

MIB Constraints

This MIB has the following constraints:

Table 3-24 DOCS-IF-MIB Constraints

MIB Object	Notes
docsIfUpstreamChannelTable	
• docsIfUpChannelWidth docsIfUpChannelSlotSize	The channel width and minislot size are related. Trying to set the channel width or minislot size separately fails if the new value is incompatible with the other parameter current setting. In addition, setting both objects together is supported only in Cisco IOS Release 12.2(15)BC2 and later releases.
docsIfCmtsMacToCmTable	Do not use GET-NEXT requests to retrieve the rows of this table, because it requires lengthy, time-consuming searches on the MAC address, which could consume excessive amounts of CPU processor time when the table is large. Instead, retrieve the individual rows using a GET request that uses the device's MAC address as the table index. This avoids possible performance problems and also ensures that the retrieved rows contain the most current, real-time data for those devices. A GET request for docsIfCmtsMacToCmTable returns NULL if the router is already processing another request for this table (either by an SNMP GET or CLI **show** command). A null string is returned if the router is processing a request for any other table that is indexed by CM or CPE MAC address, such as cdxCmCpeEntry, cdrqCmtsCmStatusTable, and docsQosCmtsMacToSrvFlowTable. Wait until the first request is done and then repeat the request for docsIfCmtsMacToCmTable.
docsIfCmtsModulationTable	

Table 3-24 DOCS-IF-MIB Constraints (continued)

MIB Object	Notes
• docsIfCmtsModGuardTimeSize • docsIfCmtsModPreambleLen	The SNMP agent might report a guard time (docsIfCmtsModGuardTimeSize) and preamble length (docsIfCmtsModPreambleLen) that do not match the values that are configured using the CLI for a particular modulation profile. This occurs when the CLI values are not appropriate for the particular PHY type and cable interface being used, and the Cisco IOS overrides the CLI values with values that are more appropriate.
docsIfCmtsTable	
• docsIfCmtsUcdInterval	Read-only.
• docsIfSigQSignalNoise	This object cannot be used with Cisco uBR-MC16S cable interface line cards when spectrum groups are configured in Cisco IOS Release 12.2(15)BC2 and earlier releases.
• docsIfUpChannelStatus	Not implemented.
• docsIfUpChannelModulationProfile	If the Cisco CMTS is configured with two modulation profiles (dynamic upstream modulation), this object returns whichever of the two profiles is currently active. This means that even if you set this object with one profile, it could return the other profile the next time it is read.
• docsIfQosProfMaxTxBurst	Deprecated and always returns NULL.
• docsIfCmtsCmStatusExtUnerroreds • docsIfCmtsCmStatusExtCorrecteds • docsIfCmtsCmStatusExtUncorrectables	Supported only in Cisco IOS Release 12.2(15)BC2 and later releases. In previous releases, these objects always return NULL.
• docsIfCmtsServiceCreateTime	Before Cisco IOS Release 12.2(15)BC1, this object displays the same creation time for all Service IDs (SIDs) for the same cable modem. In Cisco IOS Release 12.2(15)BC1 and later releases, this object shows the correct creation time for each SID.
• docsIfCmtsQosProfilePermissions	This object accurately sets the QoS profile permissions in Cisco IOS Release 12.1(20)EC, Cisco IOS Release 12.2(4)BC1, and later releases.
docsIfCmtsChannelUtilizationTable	Read-only.
• docsIfCmtsChannelUtIfType	Value is IANAifType
• docsIfCmtsChannelUtId	Value is Integer32

Table 3-24 DOCS-IF-MIB Constraints (continued)

MIB Object	Notes
• docsIfCmtsChannelUtUtilization	Value is Integer32
• docsIfCmtsChannelUtilizationInterval	Read, write.
docsIfUpstreamChannelTable	
• docsIfUpChannelPreEqEnable	
docsIfSignalQualityTable	
• docsIfSigQExtUnerroreds	Read-only. Value is 64-bit counter.
• docsIfSigQExtCorrecteds	Read-only. Value is 64-bit counter.
• docsIfSigQExtUncorrectables	Read-only. Value is 64-bit counter.
docsIfCmtsDownChannelCounterTable	Read-only.
• docsIfCmtsDownChnlCtrId	Value is Integer32
• docsIfCmtsDownChnlCtrTotalBytes	Value is Counter32
• docsIfCmtsDownChnlCtrUsedBytes	Value is Counter32
• docsIfCmtsDownChnlCtrExtTotalBytes	Value is Counter64
• docsIfCmtsDownChnlCtrExtUsedBytes	Value is Counter64
docsIfCmtsUpChannelCounterTable	Read-only.
• docsIfCmtsUpChnlCtrId	Value is Integer32
• docsIfCmtsUpChnlCtrTotalMslots	Value is Counter32
• docsIfCmtsUpChnlCtrUcastGrantedMslot	Value is Counter32
• docsIfCmtsUpChnlCtrTotalCntnMslots	Value is Counter32
• docsIfCmtsUpChnlCtrUsedCntnMslots	Value is Counter32
• docsIfCmtsUpChnlCtrExtTotalMslots	Value is Counter64
• docsIfCmtsUpChnlCtrExtUcastGrantedMslots	Value is Counter64
• docsIfCmtsUpChnlCtrExtTotalCntnMslots	Value is Counter64
• docsIfCmtsUpChnlCtrExtUsedCntnMslots	Value is Counter64

Note When using docsIfCmtsQosProfilePermissions to remove the create by modem permission from cable modems, prohibits only future activity by cable modems and deletes only unused QoS profiles that have been created by cable modems; it does not affect QoS profiles that are currently in use. This behavior is different than the **no cable qos permission modem** command, which immediately deletes QoS profiles that have been created by the cable modems and takes those modems offline.

Note The docsIfCmtsChannelUtilizationInterval attribute retains its value after a reboot even though it is not visible in the output of **show run** command.

Constraints in Cisco IOS Release 12.3(23)BC

There are no entries for the narrowband SPA downstream channels for the tables docsIfDownstreamChannelTable and docsIfCmtsDownChannelCounterTable in Cisco IOS Release 12.3(23)BC. Note that the CISCO-CABLE-WIDEBAND-MIB MIB contains narrow band information.

However, the following changes are introduced in Cisco IOS release 12.3(23)BC:

- docsIfCmtsCmStatusTable—See Table 3-25. This object points to the corresponding narrowband channel's SNMP IF index, or the Modular Cable Interface SNMP IF index.

Table 3-25 docsIfCmtsCmStatusTable

MIB Attribute	Value	Notes
docsIfCmtsCmStatusIndex	No impact	
docsIfCmtsCmStatusMacAddress	No impact	
docsIfCmtsCmStatusIpAddress	No impact	
docsIfCmtsCmStatusDownChannelIfIndex	NB channel ifindex	Return 0 if is unknown
docsIfCmtsCmStatusUpChannelIfIndex	Up channel	Return 0 if is unknown
docsIfCmtsCmStatusRxPower	No impact	
docsIfCmtsCmStatusTimingOffset	No impact	
docsIfCmtsCmStatusEqualizationData	No impact	
docsIfCmtsCmStatusValue	No impact	
docsIfCmtsCmStatusUnerroreds	No impact	
docsIfCmtsCmStatusCorrecteds	No impact	
docsIfCmtsCmStatusUncorrectables	No impact	
docsIfCmtsCmStatusSignalNoise	No impact	
docsIfCmtsCmStatusMicroreflections	No impact	
docsIfCmtsCmStatusExtUnerroreds	No impact	
docsIfCmtsCmStatusExtCorrecteds	No impact	
docsIfCmtsCmStatusExtUncorrectables	No impact	
docsIfCmtsCmStatusDocsisRegMode	No impact	
docsIfCmtsCmStatusModulationType	No impact	
docsIfCmtsCmStatusInetAddressType	No impact	
docsIfCmtsCmStatusInetAddress	No impact	
docsIfCmtsCmStatusValueLastUpdate	No impact	

DOCS-DSG-IF-MIB

This is the MIB Module for the DOCSIS Set-top Gateway(DSG). The DSG provides a one-way IP datagram transport for Out-Of-Band (OOB) messaging to cable set-top clients. The one-way IP datagram transport is called a DSG Tunnel. A DSG Tunnel carrying either a broadcast, unicast or multicast IP datagram stream originating at the DOCSIS Set-top Gateway and carrying Out-Of-Band messages intended for set-top clients. It is carried over one or more downstream DOCSIS channels. Multiple DSG tunnels may exist on a single downstream DOCSIS channel.

The following MIB tables were added with this release:

- dsgIfClassifierTable—Contains attributes use to classify inbound packets into the tunnel and classifiers for the DSG clients, encoding in the DCD messages on the downstream channels to which the classifiers apply.
- dsgIfTunnelTable—Contains group(s) of tunnel(s). Each tunnel is associated to the destination MAC address and associated to the QOS service class name.
- dsgIfTunnelGrpToChannelTable—Associates a group of tunnels to one or more downstream channel.
- dsgIfDownstreamChannelTable—Contains the associated timers, vendor specific parameters index and the channel list index to a specific downstream.
- dsgIfClientIdTable—Contains the client identification type and value. It also contains the vendor specific parameter identification.
- dsgIfVendorParamTable—Allows vendors to send specific parameters to the DSG clients within a DSG rule or within the DSG Configuration block in a DCD message.
- dsgIfChannelListTable—Contains list of one or multiple downstream frequencies that are carrying DSG tunnel(s).
- dsgIfTimerTable—Contains timers that are sent to the DSG client(s) through the DCD message.

Note DOCS-DSG-IF-MIB does not support Route Processor Redundancy Plus (RPR+) mode.

Note The DOCS-DSG-IF-MIB defines objects that are used to configure, control, and monitor the operation of the DOCSIS Set-top Gateway (DSG) 1.0 feature on Cisco uBR7200 series and Cisco uBR10012 routers. For detailed information about DOCSIS DSG, go to: http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide09186a00802065c8.html

Note The DOCS-DSG-IF-MIB top-level OID is 1.3.6.1.4.1.4491.2.1.3 (iso.org.dod.internet.private.enterprises.cableLabs.clabProject.clabProjDocsis.dsgIfMIB).

MIB Constraints

Prior to Cisco IOS Release 12.3(23)BC, there are no constraints on the DOCS-DSG-IF-MIB. (All objects listed in this MIB are implemented as defined in the MIB definition.)

Wideband Support in Cisco IOS Release 12.3(23)BC

The DOCS-DSG-IF-MIB is defined to manage DOCSIS Set-top Gateway interfaces in the following manner.

- DSG is configured on the MC interface's CGD master interface.
- A packet transmits via Multicast to the DOCSIS Set-top Gateway (DSG).
- Cisco IOS uses an IGMP configuration command to control the packets.

In Cisco IOS Release 12.3(23)BC and later, Cisco IOS no longer accepts SNMP that is mapped in the the dsgIfTunnelGrpToChannelTable on MC interface. In this circumstance, an INCONSISTENT_VALUE_ERROR system message is reported, and a corresponding error message is prompted as follows:

```
Cannot set dsg tunnel group to Modular-Cable interface, set on CGD's host downstream instead.
```

DOCS-QOS-MIB

The DOCS-QOS-MIB contains objects to configure and monitor the QoS features that are available in DOCSIS 1.1 and DOCSIS 2.0 cable networks. This MIB was published as an Internet Draft, *Data Over Cable System Interface Specification Quality of Service Management Information Base*.

The MODULE-IDENTITY for the DOCS-QOS-MIB is docsQosMIB, and its top-level OID is 1.3.6.1.2.1.10.127.7 (iso.org.dod.internet.mgmt.mib-2.transmission.docsIfMIB.docsQosMIB).

MIB Constraints and Notes

This MIB is supported only in Cisco IOS Release 12.2(4)BC1 through Release 12.2(11)BC3 to support DOCSIS 1.1 operations. The MIB is deprecated in later releases to conform with the DOCSIS 2.0 specifications.

Table 3-26 DOCS-QOS-MIB Constraints

MIB Object	Notes
docsQosCmtsMacToSrvFlowTable	Do not use GET-NEXT requests to retrieve the rows of this table, because it could require lengthy, time-consuming searches on the MAC address, which could consume excessive amounts of CPU processor time when the table is large. Instead, retrieve the individual rows using a GET request that uses the device's MAC address as the table index. This avoids possible performance problems and also ensures that the retrieved rows contain the most current, real-time data for those devices. A GET request for docsQosCmtsMacToSrvFlowTable returns NULL if the router is already processing another request for this table (either by an SNMP GET or CLI **show** command). A null is also returned if the router is processing a request for any other table that is indexed by CM or CPE MAC address, such as cdxCmCpeEntry, cdrqCmtsCmStatusTable, and docsIfCmtsMacToCmTable. Wait until the first request is done and then repeat the request for docsQosCmtsMacToSrvFlowTable.
docsQosParamSetTable	This table describes the set of DOCSIS 1.1 QOS parameters defined in a managed device.
• docsQosParamSetMaxTrafficBurst	Valid only for Best Effort, non-Real-Time Polling, and Real-Time Polling bursts. For all other bursts, this object reports 0.

Table 3-26 DOCS-QOS-MIB Constraints (continued)

MIB Object	Notes
• docsQosServiceClassDirection • docsQosServiceClassSchedulingType	These objects must be set together as part of the same SET request when configuring a downstream service class.
• docsQosParamSetEntry**	Identifies a unique set of QoS parameters.
docsQosServiceFlowStatsTable	Reports the downstream traffic counters for cable modems that are provisioned for DOCSIS 1.1 and DOCSIS 2.0 operation. For DOCSIS 1.0 cable modems, use the cdxCmtsServiceExtTable in CISCO-DOCS-EXT-MIB.
• docsQosServiceFlowStatsEntry**	Describes a set of service flow statistics. An entry in the table exists for each Service Flow ID. The ifIndex is an ifType of docsCableMaclayer(127)."
docsQosPHSTable	This table describes set of payload header suppression entries.
• docsQosPHSEntry**	
docsQosPktClassTable	
• docsQosPktClassEntry**	An entry in this table that provides a single packet classifier rule.
docsQosServiceFlowTable	
• docsQosServiceFlowEntry**	Describes a service flow. An entry in the table exists for each Service Flow ID. The ifIndex is an ifType of docsCableMaclayer(127).
docsQosUpstreamStatsTable	
• docsQosUpstreamStatsEntry**	Describes a set of upstream service flow statistics.
docsQosServiceFlowLogTable	Logs deleted DOCSIS 1.1 and DOCSIS 2.0 service flows, but this table does not contain any information until after logging is specifically enabled using the **cable sflog** command in global configuration mode.
docsQosDynamicServiceStatsTable	(not applicable for Docsis 1.0 modems)
• docsQosDCCReqs	Read-only.The number of Dynamic Channel Change Request messages traversing an interface. This count is nonzero only on downstream direction rows.
• docsQosDCCRsps	Read-only. The number of Dynamic Channel Change Response messages traversing an interface. This count is nonzero only on upstream direction rows.
• docsQosDCCAcks	Read-only. The number of Dynamic Channel Change Acknowledgement messages traversing an interface. This count is nonzero only on downstream direction rows.
• docsQosDCCs	Read-only. The number of successful Dynamic Channel Change transactions. This count is nonzero only on downstream direction rows.

Table 3-26 DOCS-QOS-MIB Constraints (continued)

MIB Object	Notes
• docsQosDCCFails	Read-only. The number of failed Dynamic Channel Change transactions. This count is nonzero only on downstream direction rows.

**The SNMP query sessions have been improved in these tables.

Note For detailed information about load balancing and dynamic channel change on CMTS, go to the following URL:
http://www.cisco.com/en/US/docs/cable/cmts/troubleshooting_batch9/cmtslbg.html

DOCS-SUBMGT-MIB

The DOCS-SUBMGT-MIB contains objects to configure and monitor the subscriber management features in DOCSIS 1.1 and DOCSIS 2.0 cable networks. These objects include packet filtering and CPE device control, and help protect the cable network from intentional or accidental misuse by subscribers.

This MIB was published as an Internet Draft, *Management Information Base for Data Over Cable Service Interface Specification (DOCSIS) Cable Modem Termination Systems for Subscriber Management*.

The MODULE-IDENTITY for the DOCS-SUBMGT-MIB is docsSubMgt, and its top-level OID is 1.3.6.1.3.83.4 (iso.org.dod.internet.experimental.83.docsSubMgt). Because this is an experimental MIB, its top-level OID is expected to change when the specifications are finalized.

MIB Constraints

This MIB has the following constraints:

- The Cisco uBR10012 router does not support the packet filtering objects in this MIB.
- Supported only in Cisco IOS Release 12.2BC and later releases that support DOCSIS 1.1 and DOCSIS 2.0 operations.
- The Cisco uBR-MC16U/X and Cisco uBR-MC28U/X cable interface line cards support this MIB and its objects only in Cisco IOS Release 12.2(15)BC1 and later releases.

Table 3-27 DOCS-SUBMGT-MIB Constraints

MIB Object	Notes
docsSubMgtCpeIpTable	CPE devices listed for a particular cable modem are not automatically cleared when the cable modem is reset. If a problem occurs, then set the docsSubMgtCpeControlReset object to True for that particular cable modem to erase all of its CPE entries.
• docsSubMgtCpeControlMaxCpeIp	This object can be overridden by the **cable modem max-cpe** command in global configuration mode.

DTI-MIB

The DTI-MIB supports the RF Gateway with these MIB attributes and values for the :

- dtiProtocolEntityType—Refer to Table 3-28.
- dtiPathTraceabilityTable—Refer to Table 3-29.
- entPhysicalTable—Refer to these tables:
  - Table 3-30—entPhysicalTable Entries for the Cisco DTI Card
  - Table 3-30—entPhysicalTable Entries for Cisco DTI Ports
  - Table 3-31—entAliasMappingTable Entries for DTI Interfaces

Table 3-28 dtiProtocolEntityType Entries

MIB Attribute	Value	Notes
dtiProtocolEntityType	root(1), server(2), client(3)	
dtiProtocolClientClockType	ituI(1), ituII(2), ituIII(3), st3(4), dtiClock(5)	
dtiProtocolServerStatusFlag	unknown(0), warmup(1), freerun(2), fastTrackingMode(3), normalMode(4), holdoverMode(5), clientStable(6), testMode(7)	Server status
dtiProtocolClientStatusFlag	unknown(0), warmup(1), freerun(2), fastTrackingMode(3), normalMode(4), holdoverMode(5), bridgingMode(6), testMode(7)	Client status
dtiProtocolServerToDState	Valid(1) or Invalid(2)	Validity of TOD
dtiProtocolServerToDType	Default(1), userTime(2), ntpv4(3), gps(4)	Current TOD source for DTI connection
dtiProtocolServerToDValue	String	Value of TOD in format DDDDD.YYYY/MM/DD.HH:MM:SS.SHH:F.D
dtiProtocolServerCableAdvanceFlag	Valid(1), invalid(2), manual(3)	Cable advance status
dtiProtocolServerCableAdvanceValue	String	Cable advance value
dtiProtocolClientPhaseError	Signed number	Phase error counter
dtiProtocolClientVersion	Unsigned number	Client DTI version
dtiProtocolClientPathTraceability	Unsigned number	DTI tracibility
dtiProtocolServerClientStableFlag	Valid(1) or Invalid(2)	Client performance stable status of DTI server frame

Table 3-29 dtiPathTraceabilityTable Entries

MIB Attribute	Value	Notes
dtiPathTraceabilityIndex	Unsigned number	index
dtiPathTraceabilityRootServerInetAddrType	unknown(0), ipv4(1), ipv6(2), ipv4z(3), ipv6z(4), dns(16)	Server address type
dtiPathTraceabilityRootServerInetAddr	<IP address>	Server address
dtiPathTraceabilityRootServerOutPhyIdx	Physical index	
dtiPathTraceabilityServerInetAddrType	unknown(0), ipv4(1), ipv6(2), ipv4z(3), ipv6z(4), dns(16)	
dtiPathTraceabilityServerInetAddr	<IP address>	
dtiPathTraceabilityServerOutPhyIdx	Physical index	
dtiPathTraceabilityRootServerProtVersion		DTI version
dtiPathTraceabilityServerProtVersion		DTI protocol version

MIB Constraints

This MIB is supported in Cisco IOS Release 12.3(23)BC and later releases.

ENTITY-MIB

The ENTITY-MIB represents physical and logical entities (components) in the router and allow SNMP management of those entities. This MIB was released as RFC 2737, *Entity MIB (Version 2)*.

The MIB table entPhysicalTable identifies the physical entities in the router. The entPhysicalTable contains a single row for the 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 run time, based on the actual router configuration.

The ENTITY-MIB shows information only about hardware devices, not virtual devices.

The MODULE-IDENTITY for the ENTITY-MIB is entityMIB, and its top-level OID is 1.3.6.1.2.1.47 (iso.org.dod.internet.mgmt.mib-2.entityMIB).

MIB objects and related constraints introduced in Cisco IOS Release 12.3(23)BC are included in Table 3-33.

MIB Constraints

Table 3-30 entPhysicalTable Entries for the DTI Line Card in Cisco IOS Release 12.3(23)BC

MIB Attribute	Value	Notes
entPhysicalIndex	Physical index	Cisco IOS Release 12.3(23)BC. Set by Entity MIB when instance is created
entPhysicalDescr	UBR10-DTCC for Fireballs, UBR10-DTCC for EightBells.	Cisco IOS Release 12.3(23)BC. Eightbell is the current value.
entPhysicalVendorType	cevUbrTccPlus for Fireballs, cevUbrDtcc for Eightbells	Cisco IOS Release 12.3(23)BC.
entPhysicalContainedIn	Corresponding chassis index	Cisco IOS Release 12.3(23)BC.
entPhysicalClass	`module`	Cisco IOS Release 12.3(23)BC.
entPhysicalParentRelPos	A number denotes where the TCC w/ DTI card locates.	Cisco IOS Release 12.3(23)BC.
entPhysicalName	uBR10k DTI port slot/subslot.	Cisco IOS Release 12.3(23)BC.
entPhysicalHardwareRev	Hardware revision	Cisco IOS Release 12.3(23)BC. Read from EEPROM
entPhysicalFirmwareRev	Firmware revision	Cisco IOS Release 12.3(23)BC. Read from EEPROM
entPhysicalSoftwareRev	Software revision	Cisco IOS Release 12.3(23)BC. Read from EEPROM
entPhysicalSerialNum	N/A	Cisco IOS Release 12.3(23)BC. Read from EEPROM
entPhysicalMfgName	Cisco	Cisco IOS Release 12.3(23)BC.
entPhysicalModelName	UBR10-TCC+-T1 for FireBalls, UBR10-DTCC for Eightbells.	Cisco IOS Release 12.3(23)BC.
entPhysicalAlias		Cisco IOS Release 12.3(23)BC. Null by default, can be set.
entPhysicalAssetID		Cisco IOS Release 12.3(23)BC. Null by default, can be set.
entPhysicalIsFRU	TRUE(1)	Cisco IOS Release 12.3(23)BC.

Table 3-31 entPhysicalTable Entries for the DTI Ports in Cisco IOS Release 12.3(23)BC

MIB Attribute	Value	Notes
entPhysicalIndex	Physical index	Set when the port is enabled.
entPhysicalDescr	uBR1000 DTI 10BaseT like port	
entPhysicalVendorType	cevPortBaseTEther	Applying, will give update later.
entPhysicalContainedIn	DTI card physical index	e.g. Ge containedin SFP module
entPhysicalClass	Port(10)	

Table 3-31 entPhysicalTable Entries for the DTI Ports in Cisco IOS Release 12.3(23)BC (continued)

MIB Attribute	Value	Notes
entPhysicalParentRelPos	0	A number given when DTI is enabled, increasing from 0.
entPhysicalName	uBR10k DTI port <slot>/<subslot>/<unit>	
entPhysicalHardwareRev	N/A	
entPhysicalFirmwareRev	N/A	
entPhysicalSerialNum	N/A	
entPhysicalMfgname	Cisco	
entPhysicalModelname	N/A	
entPhysicalAlias	NA	
entPhysicalAssetID	NA	
entPhysicalIsFRU	False(2)	

Table 3-32 entAliasMappingTable Entries for DTI interfaces

MIB Attribute	Value	Notes
entAliasLogicalIndexOrZero	0	Logical index.
entAliasMappingIdentifier	ifIndex.<ifIndex#>	ifindex# is corresponding DTI interface's index.

Table 3-33 ENTITY-MIB Constraints Prior to Cisco IOS Release 12.3(23)BC

MIB Object	Notes
entPhysicalTable	This table does not include the NPE on the Cisco uBR7200 series routers until Cisco IOS Release 12.2(8)BC1 and later releases.
• entPhysicalFirmwareRev	Not implemented.
• entPhysicalAlias	Not implemented.
• entPhysicalAssetID	Not implemented.
• entPhysicalSoftwareRev	Supported only in Cisco IOS Release 12.2(8)BC2 and later releases.
• entPhysicalHardwareRev • entPhysicalModelName • entPhysicalSerialNumber	Supported only for some cards. In addition, entPhysicalSerialNumber displays the correct serial number only in Cisco IOS Release 12.1(20)EC, 12.2(15)BC2, and later releases.
• entPhysicalHardwareRev	• Supports the Cisco Unique Device Identifier (UDI). • Contains the Version Identifier (VID).
• entPhysicalModelName	• Supports the Cisco Unique Device Identifier (UDI). • Contains the orderable Product Identifier (PID).

Table 3-33 ENTITY-MIB Constraints Prior to Cisco IOS Release 12.3(23)BC (continued)

MIB Object	Notes
• entPhysicalSerialNumber	• Supports the Cisco unique device Identifier (UDI). • Contains the hardware Serial Number (SN). Note that for non-UDI compliant hardware, these fields might contain a NULL string. Currently, the UDI support is not implemented for the standby PRE. For standby PRE, both entPhysicalHardwareRev and entPhysicalSerialNumber will contain NULL string.
• entPhysicalIsFRU	• Supported on the Cisco uBR7100 series and Cisco uBR7200 series routers in all releases. • Supported on the Cisco uBR10012 router only in Cisco IOS Release 12.2(11)BC2 and later releases.
• entPhysicalDescr	This object describes the Cisco uBR10012 router either as UBR10000 or UBR10012, depending on Cisco IOS release.
• entPhysicalContainedIn	This object accurately displays the location of the FastEthernet network management port on the active PRE-1 module only in Cisco IOS Release 12.2(4)BC1b and later releases.
entLPMappingTable	Not implemented.
entAliasMappingTable	• On Cisco uBR10012 routers, this table does not contain entries for the TCC+ cards. • On Cisco uBR10012 routers with two redundant PRE modules installed, the entPhysicalDesc entries in the entAliasMappingTable contain two sets of apparently identical references for each PRE module to "Forwarding Processor," "Routing Processor," and "Network Management Ethernet" (the Fast Ethernet port on the PRE modules). This occurs because two PRE modules are installed in the chassis, but only one is active. So the SNMP agent points both entries to the same PRE module. • The entAliasMappingTable supports virtual interfaces only in Cisco IOS Release 12.2(15)BC2 and later releases. The entries in this table show the logical upstream interface (as defined by ifIndex from the IF-MIB) that is using each physical upstream connector. This support also slightly changed the parent-child relationships of the ports on cable interface line cards, as described in the next section, "Changes to Support Virtual Interfaces".

The entPhysicalTable and entAliasMappingTable objects are automatically updated whenever a card is removed or inserted into a slot or when you enter a command at the CLI prompt that affects the operation of the card.

Cisco uBR100012 SPA-24XWBD-SFP Shared Port Adapter

Table 3-34 lists physical entities and values for the Cisco uBR100012 CMTS SPA-24XWBD-SFP.

Table 3-34 entPhysicalTable Objects for Cisco Ubr100012 SPA-24XWBD-SFP

entPhysicalDescr	entPhysical-Class	entPhysicalVendor-Type	entPhysicalName	entPhysical/IsFRU
SPA Bay Container	container	cevContainerSPABay	“ ”(null)	
uBR10KSPA Card	Module(9)	cevSpa24xWbdSfp	SPA-WB Wideband CMTS SPA 3/00	True(1) (represents a field re-placeable unit)
Pluggable Optics Container	container	cevContainerSFP	“ ”(null)	
Short wavelength gigabit Ethernet SFP	Port(10)	cevSFP1000BaseSx	SFP slot/sub-slot/unit/port Where port can be 0 or 1. For example, SFP 3/0/0/1	True(1)
Long wavelength gigabit Ethernet SFP	Port(10)	cevSFP1000BaseLx	SFP slot/sub-slot/unit/port Where port can be 0 or 1. For example, SFP 3/0/0/1	True(1)
Copper gigabit Ethernet SFP	Port(10)	cevSFP1000BaseT	SFP slot/sub-slot/unit/port Where port can be 0 or 1. For example, SFP 3/0/0/1	True(1)
Extended reach gigabit Ethernet SFP 1000BaseZx	Port(10)	cevSFP1000BaseZx	SFP slot/sub-slot/unit/port Where port can be 0 or 1. For example, SFP 3/0/0/1	True(1)

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 Identifying Cisco Unique Device Identifiers, page A-41 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)

Overview of the ENTITY-MIB

The following are the most important objects in the ENTITY-MIB for the management of physical entities on the router:

- entPhysicalTable—Describes each physical component (entity) in the router. The table contains a row entry for the top-most entity (the chassis) and then for each entity in the chassis. Each entry provides the name and description of the entry, its type and vendor, and a description of the reason how the entity was first entered into the containment tree.
- entPhysicalIndex—Uniquely identifies each entry. This value is guaranteed to be unique across all equipment in this chassis and across all MIBs, allowing you to correlate the data from several MIBs for any particular entity.

- entAliasMappingTable—Maps each physical port's entPhysicalIndex value to the corresponding ifIndex value in the ifTable in the IF-MIB. This provides a quick way of identifying a particular port with a particular interface.

  In Cisco IOS Release 12.2(15)BC2 and later releases, the entAliasMappingTable also shows the mapping of physical upstream connectors to logical upstream interface when virtual interfaces are configured on the Cisco uBR-MC5X20S and Cisco uBR-MC5X20U cable interface line cards. This support also changed the parent-child relationships of cable interface line cards and their ports. For more information, see the "Changes to Support Virtual Interfaces" section on page 3-76.

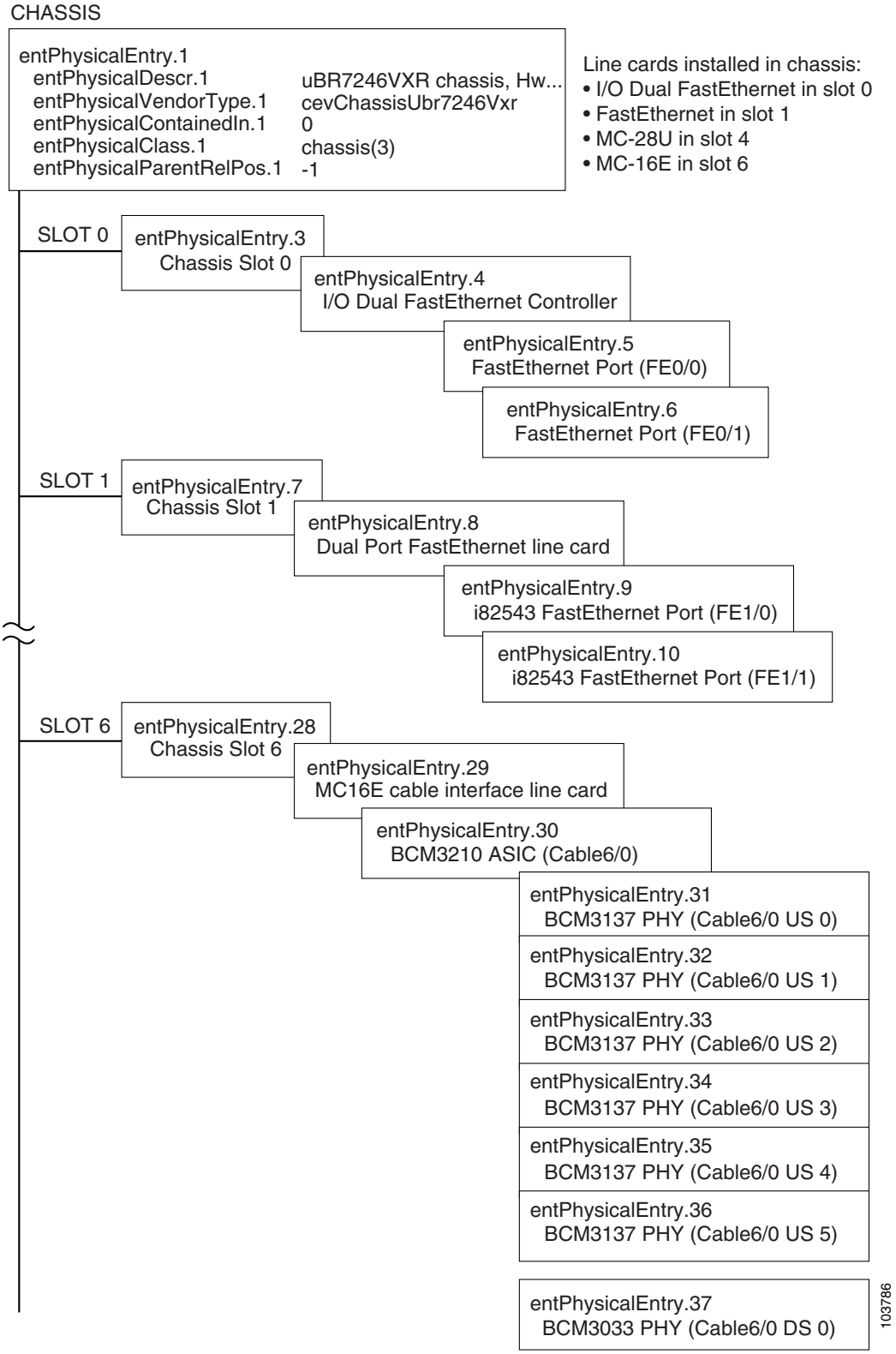
- entPhysicalContainsTable—For each physical entity, lists the entPhysicalIndex value for any child objects of the entity. This provides an easy way of creating the container tree for the router, which shows the relationship between physical entities in the chassis.

  Typically, the container tree is organized as follows:

  - The chassis is the top-most level and contains the processor card and chassis slots.
  - Chassis slots contain the individual line cards and I/O controller (if installed).
  - Line cards contain ports (interfaces).
  - Cable interface line cards contain downstream ports (known as cable line card). In Cisco IOS Release 12.2(15)BC1 and earlier releases, each downstream port then contains the upstream ports that are associated with it. In Cisco IOS Release 12.2(15)BC2 and later releases, the downstream ports and upstream are all children of the cable interface line card.

Figure 3-1 shows an overview of the arrangement of objects in a Cisco uBR7246VXR router, with one Fast Ethernet line card and two cable interface line cards. (This graphic shows the cable interface line cards as they are represented in Cisco IOS Release 12.2(15)BC1 and earlier releases.)

Figure 3-1 ENTITY-MIB for Cisco uBR7246VXR Chassis



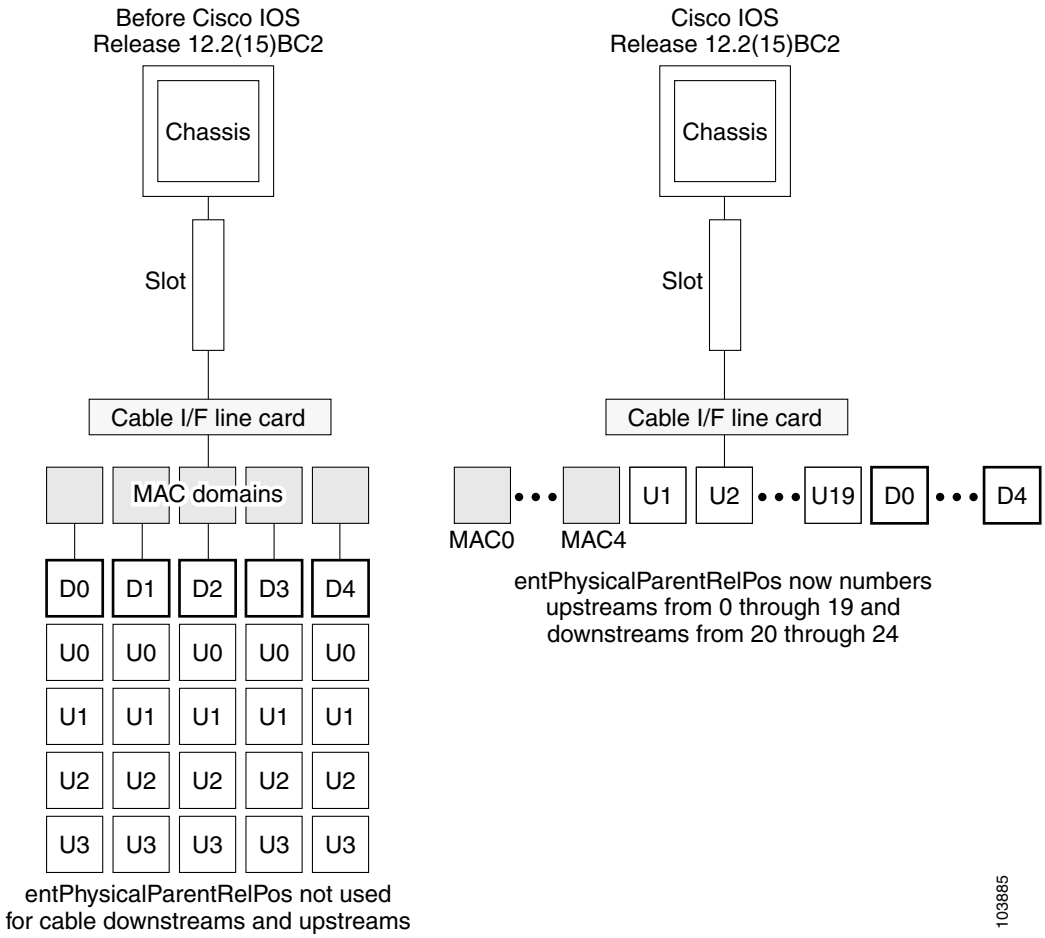
Changes to Support Virtual Interfaces

To enable SNMP support for Virtual Interfaces, Cisco IOS Release 12.2(15)BC2 changed how the entPhysicalTable in the ENTITY-MIB displays the information for cable interface line cards. Previously, the cable interface line card was the parent to one or more MAC domains, and each MAC domain then was the parent to one downstream and one or more upstreams.

Because an upstream can now be associated with any MAC domain and downstream in Cisco IOS Release 12.2(15)BC2, the ENTITY-MIB no longer associates upstreams and downstreams with specific MAC domains, but instead shows all of them as being children of the line card. The entityPhysicalParentRelPos also now numbers the upstreams in sequential order, followed by the downstreams, so that on the Cisco uBR-MC5X20S cards, the upstreams are numbered from 0 to 19, and the downstreams from 20 to 24.

Figure 3-2 shows the difference in how the entPhysicalTable in the ENTITY-MIB organized a Cisco uBR-MC5X20S cable interface line card in previous releases and in Cisco IOS Release 12.2(15)BC2. For consistency, all cable interface line cards use this approach, even if they do not support the Virtual Interfaces feature.

Figure 3-2 ENTITY-MIB Changes for Virtual Interface Support on Cable Interface Line Cards



The mapping between the physical upstream connectors and the logical upstream interfaces is shown in the entityAliasMappingTable. Each entry in this table contains the ifDescr index (as defined in the ifTable in the IF-MIB) that maps to the physical connector that is being used for that interface. The entityAliasMappingTable is automatically updated to show the mapping between the physical upstream connectors and the logical interfaces whenever the **cable upstream connector** command used.

Chassis Slot Layout

Table 3-35 provides information about the entities contained in chassis slots on the Cisco uBR10012 router.

Table 3-35 Cisco uBR10012 Router Chassis Slot Contents

Entity	Can Contain	Notes
Slots 1 to 8	One full-size line card per slot.	For chassis slot containers: • entPhysicalContainedIn is always 1 (which is the entPhysicalIndex of the chassis, which contains all chassis slots). • entPhysicalParentRelPos is different for each chassis slot, to show its position in the chassis. The Cisco uBR10012 router supports only full-size line cards in chassis slots: • entPhysicalContainedIn is different for each line card (because each line card is installed in a different chassis slot). • entPhysicalParentRelPos is always 1 (only one card per slot).
Slots A and B	One route processor (RP) per slot.	Router can have two RPs (one for each PRE installed in slot A and slot B). Each RP contains: FP NME Core temperature sensor Inlet temperature sensor Flash card slots (2), which are not modeled in the ENTITY MIB.
	One forwarding processor (FP) per slot.	Router can have two FPs (one for each PRE installed in slot A and slot B).

ETHERLIKE-MIB

The ETHERLIKE-MIB contains objects to manage Ethernet-like interfaces on the router. This MIB was released as RFC 2665, *Definitions of Managed Objects for the Ethernet-like Interface Types*.

The MODULE-IDENTITY for the ETHERLIKE-MIB is etherMIB, and its top-level OID is 1.3.6.1.2.1.35 (iso.org.dod.internet.mgmt.mib-2.etherMIB).

MIB Constraints

Table 3-36 lists the ETHERLIKE-MIB constraints.

Table 3-36 ETHERLIKE-MIB Constraints

MIB Object	Notes
dot3StatsTable	
• dot3StatsCarrierSenseErrors	Implemented starting in Cisco IOS Release 12.2(15)BC2 and later releases. It returns NULL in earlier releases.
• dot3StatsSQETestErrors	Not implemented and is always 0.
• dot3StatsInternalMacTransmitErrors	Not implemented and is always 0.
• dot3StatsEtherChipSet	Deprecated and is always NULL
• dot3StatsFrameTooLongs	For Fast Ethernet interfaces and for Gigabit Ethernet interfaces, this object counts only frames of 1545 bytes or larger (not counting the cyclic redundancy check [CRC]), regardless of the maximum transmission unit (MTU) value.
dot3CollTable	Not implemented.

EVENT-MIB

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

The MODULE-IDENTITY for the EVENT-MIB is dismanEventMIB, and its top-level OID is 1.3.6.1.2.1.88 (iso.org.dod.internet.mgmt.mib-2.dismanEventMIB).

MIB Constraints

This MIB is:

- Not supported in any Cisco IOS Release 12.1EC software image.
- Supported in all Cisco IOS Release 12.2BC software images for the Cisco uBR10012 router.
- Supported only in Cisco IOS Release 12.2BC "-is-" software images in Cisco uBR7100 series and Cisco uBR7200 series routers.

EXPRESSION-MIB

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

The MODULE-IDENTITY for the EXPRESSION-MIB is expressionMIB, and its top-level OID is 1.3.6.1.4.1.9.10.22 (iso.org.dod.internet.private.enterprises.cisco.ciscoExperiment.expressionMIB).

MIB Constraints

There are no constraints on this MIB.

HC-RMON-MIB

The HC-RMON-MIB contains objects that provide high capacity (HC) information that supplements the remote monitoring objects in the RMON-MIB and the RMON2-MIB.

The MODULE-IDENTITY for the HC-RMON-MIB is hcRMON, and its top-level OID is 1.3.6.1.2.1.16.20.8 (iso.org.dod.internet.mgmt-mib-2.rmon.rmonConformance.hcRMON).

MIB Constraints

These are no constraints on this MIB.

IF-MIB

The IF-MIB describes the attributes of physical and logical interfaces. The router supports the ifGeneralGroup of MIB objects for all layers (ifIndex, ifDescr, ifType, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, ifLastChange, ifName, ifLinkUpDownTrapEnable, ifHighSpeed, and ifConnectorPresent). This MIB was released as RFC 2233, *The Interfaces Group MIB Using SMIv2*.

In Cisco IOS Release 12.2(15)BC1c and later releases, the Cisco CMTS routers implemented a cache to allow continuous polling of the ifTable interface counters, without creating spikes in the CPU usage. The cache is updated approximately every 10 seconds, which means that if you read the counter more quickly than that, the SNMP request might not return a new value.

The counters do continue to increment, however, to account for the actual traffic occurring on the interfaces, and another SNMP request in 10 seconds will show the new values. However, the use of the cache means that the counters displayed by the **show interface** command might not exactly match the values returned by the ifTable interface counters.

Also, you can retrieve interface packet counters for both a cable interface and for the corresponding downstream. When using an ifIndex that points to a downstream (the ifDescr shows "cX/Y/Z-downstream"), the packet counters include not only the data packets but also the DOCSIS MAC-layer packets that are transmitted on that downstream. To retrieve counters for only the data packets (which corresponds to the output from the **show interface** command), use the ifIndex for the interface itself (the ifDescr shows "cX/Y/Z").

The MODULE-IDENTITY for the IF-MIB is ifMIB, and its top-level OID is 1.3.6.1.2.1.31 (iso.org.dod.internet.mgmt.mib-2.ifMIB).

IF-MIB Notes

Note The IF-MIB does not contain any information about cable subinterfaces.

Note It is expected that the interface counters displayed by the **show interface** command might not exactly match the values returned by the ifTable interface counters.

Table 3-36 lists the IF-MIB constraints and notes.

Table 3-37 IF-MIB Notes

MIB Object	Notes
ifXEntryTable	
• ifAlias	Supported for non-cable interfaces on the Cisco uBR10012 router in Cisco IOS Release 12.2(11)BC2 and later releases. Supported for cable interfaces only in Cisco IOS Release 12.2(15)BC2 and later releases.
IfTable	
• ifDescr	On the Cisco uBR10012 router, the first ifDescr object is typically "Ethernet0/0/0," which is the internal backplane Ethernet interface that the PRE module uses to communicate with the line cards and the secondary PRE module (if installed). This interface cannot be configured or otherwise used, and therefore should be ignored. Separate ifDescr entries appear for each cable interface upstream and downstream. These entries have an "upstream" or "downstream" suffix. In addition, an ifDescr entry exists for the cable interface itself (without an "upstream" or "downstream" suffix). This entry represents the MAC-layer interface on the cable interface. Note that ifDescr supports Virtual Interfaces only in Cisco IOS Release 12.2(15)BC2 and later releases. Also see the ENTITY-MIB for entAliasMappingTable support.
• ifType	Always reports a value of 6 (Ethernet interface) for Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces. This conforms with the recommendations of RFC 2665, and accommodates 10/100/1000 interfaces that negotiate the link speed with the remote end.
• ifInOctets • ifOutOctets	You must use Cisco IOS Release 12.2(11)BC3 or a later release for these objects to reliably count the octets on cable interfaces.
• ifSpeed	For cable interfaces, this object has valid values only for the upstream and downstream ifDescr entries. The ifSpeed for the MAC-layer cable interface entry is always 0.
• ifInUcastPkts • ifOutMulticast	These objects count both data packets and MAC-layer request packets from cable modems on an upstream, so as to conform to RFC 2670.
• ifHCInUcastPkts • ifHCInBroadcastPkts • ifHCOutUcastPkts	Supported only in Cisco IOS Release 12.2(15)BC2 and later releases.
• ifInUnknownProtos	This object can double-count packets in some circumstances before Cisco IOS Release 12.2(11)BC2.

IF-MIB Notes for Cisco IOS Release 12.3(23)BC

IF-MIB Supported Traps

Cisco IOS Release 12.3(23)BC enables you to shut down the narrowband downstream ports of a Shared Port Adaptor (SPA) with the **shutdown** command. The following traps are supported:

- LinkDown
- LinkUp

When an interface is shut down, or enabled with the **no shutdown** command, traps are sent for each individual channel. The GigE interfaces are not included in this event, and there is no statistical data available per interface for these GigE ports.

Cisco IOS Release 12.3(23)BC introduces support for new narrowband virtual interfaces, and the modular-cable interface. The RF channels are logical channels that represent external QAMs. The RF channels do not represent an interface, but the narrowband channel represents a logical identity of cable interfaces.

The two GigE ports of the Shared Port Adapter are not supported in the IF-MIB for these reasons. However, the following tables are supported:

- ifTable
- ifXTable
- ifStackTable

Table 3-38 ifTable Entries for NB channels

MIB Attribute	Value	Notes
ifIndex	index, unsigned integer	A unique value for each interface, greater than zero, remains constant between initializations.
ifDescr	Modular-Cable[slot#]/[subslot#]/[unit#]:[Chan#]	
ifType	other	Use "other" for downstream
ifMtu	1500	c.f. IF-MIB
ifSpeed	NA	RFC2670 requires 0 for Cable MAC layer ifSpeed
ifPhysAddress	MAC Address	
ifAdminStatus	Up/Down	It presents shut/no-shut of the narrowband downstream narrowband channel. It will always be Down unless Admin Status is Up, corresponding RF channel is configured and the Modular-Cable interface is configured.
ifOperStatus	Up/Down	It will always be Down unless Admin Status is Up and corresponding RF channel and the Modular-Cable interfaces are configured.
ifLastChange	Timeticks	c.f. IF-MIB
ifInOctets	NA - Only out supported	In counter not supported
ifInUCastPkts	NA - Only out supported	In counter not supported

Table 3-38 ifTable Entries for NB channels (continued)

MIB Attribute	Value	Notes
ifInNUcastPkts	NA - Only out supported	In counter not supported
ifInDiscards	NA - Only out supported	In counter not supported
ifInErrors	NA - Only out supported	In counter not supported
ifInUnknownProtos	NA - Only out supported	In counter not supported
ifOutOctets	Counter Value	c.f. IF-MIB
ifOutUcastPkts	Counter Value	c.f. IF-MIB
ifOutNUcastPkts	Deprecated	c.f. IF-MIB
ifOutDiscards	Counter Value - Not Supported	c.f. IF-MIB
ifOutErrors	Counter Value - NA	c.f. IF-MIB
ifOutQLen	Deprecated	c.f. IF-MIB
ifSpecific	Deprecated	c.f. IF-MIB

Table 3-39 ifXTable Entries for NB channels

MIB Attribute	Value	Notes
ifName	Mo[slot#]/[subslot#]/[unit#]:[Chan#]	
ifInMulticastPkts	NA - Only out supported	In counter not supported
ifInBroadcastPkts	NA - Only out supported	In counter not supported
ifOutMulticastPkts	NA	c.f. IF-MIB
ifOutBroadcastPkts	NA	c.f. IF-MIB
ifHCInOctets	NA - Only out supported	In counter not supported
ifHCInUcastPkts	NA - Only out supported	In counter not supported
ifHCInMulticastPkts	NA - Only out supported	In counter not supported
ifHCInBroadcastPkts	NA - Only out supported	In counter not supported
ifHCOutOctets	Counter Value	c.f. IF-MIB
ifHCOutUcastPkts	Counter Value	c.f. IF-MIB
ifHCOutMulticastPkts	NA	c.f. IF-MIB
ifHCOutBroadcastPkts	NA	c.f. IF-MIB
ifLinkUpDownTrapEnable	enable(1)/disable(2)	enabled by default
ifHighSpeed	NA - same as ifSpeed	RFC2670 requires 0 for Cable MAC layer ifSpeed.
ifPromiscuousMode	false(2)	always set to false
ifConnectorPresent	false(2)	always set to false
ifAlias	Description string	
ifCounterDiscontinuityTime	Timeticks	c.f. IF-MIB

Table 3-40 ifStackTable Entries for NB channel

MIB Attribute	Value	Notes
ifStackHigherLayer	ifIndex or zero	ifIndex or zero
ifStackLowerLayer	zero	ifIndex or zero, return always zero
ifStackStatus	active	not allowed for set, return always active

IGMP-MIB

The IGMP-MIB contains objects to manage the Internet Group Management Protocol (IGMP) on the router. This MIB was published as an experimental Internet Draft that has since been replaced by the IGMP-STD-MIB.

The MODULE-IDENTITY for the IGMP-MIB is igmpMIB, and its top-level OID is 1.3.6.1.3.59 (iso.org.dod.internet.experimental-2.igmpMIB).

MIB Constraints

This MIB is supported only in Cisco IOS Release 12.1EC and only for the Cisco uBR7100 series and Cisco uBR7200 series routers. In other releases, this MIB is deprecated and replaced by the IGMP-STD-MIB (RFC 2933).

IGMP-STD-MIB

The IGMP-STD-MIB contains objects to manage the Internet Group Management Protocol (IGMP) on the router. This MIB was released as RFC 2933*, Internet Group Management Protocol MIB*, and replaces the IGMP-MIB that was supported in earlier releases.

The MODULE-IDENTITY for the IGMP-STD-MIB is igmpStdMIB, and its top-level OID is 1.3.6.1.2.1.85 (iso.org.dod.internet.mgmt.mib-2.igmpStdMIB).

MIB Constraint

This MIB is supported only in Cisco IOS Release 12.2BC and later releases.

INT-SERV-MIB

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

The MODULE-IDENTITY for the INT-SERV-MIB is intSrv, and its top-level OID is 1.3.6.1.2.1.52 (iso.org.dod.internet.mgmt.mib-2.intSrv).

MIB Constraints

There are no constraints on this MIB.

IP-MIB

The IP-MIB contains objects to display classless interdomain routing (CIDR) multipath IP routes. This MIB was initially defined as part of RFC1213-MIB and then later released as RFC 2011, *SNMPv2 Management Information Base for the Internet Protocol Using SMIv2*.

In RFC1213-MIB, the MODULE-IDENTITY for the IP-MIB is ipMIB, and its top-level OID is 1.3.6.1.2.1.4 (iso.org.dod.internet.mgmt.mib-2.ipMIB). In RFC 2011, its top-level OID is 1.3.6.1.2.1.48 (iso.org.dod.internet.mgmt.mib-2.ipMIB).

MIB Constraint

The Cisco CMTS routers support the RFC1213-MIB version of this MIB (1.3.6.1.2.1.4).

IPMROUTE-MIB

The IPMROUTE-MIB contains objects to monitor and configure the operation of IP multicast routing on the router. This MIB was published as an experimental Internet Draft that has since expired and has been replaced by the IPMROUTE-STD-MIB.

The MODULE-IDENTITY for the IPMROUTE-MIB is ipMRoute, and its top-level OID is 1.3.6.1.3.60 (iso.org.dod.internet.experimental.ipMRoute).

MIB Constraint

This MIB is supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers.

IPMROUTE-STD-MIB

The IPMROUTE-STD-MIB contains objects to monitor and configure the operation of IP multicast routing on the router. This MIB was released as RFC 2932, *IPv4 Multicast Routing MIB*, and replaces the IPMROUTE-MIB that was supported in earlier releases.

The MODULE-IDENTITY for the IPMROUTE-STD-MIB is ipMRouteStdMIB, and its top-level OID is 1.3.6.1.2.1.83 (iso.org.dod.internet.mgmt.mib-2.ipMRouteStdMIB).

MIB Constraint

This MIB is not supported on the Cisco uBR10012 router.

ISDN-MIB

The ISDN-MIB contains objects to monitor and configure the ISDN interfaces, both Basic Rate Interface (BRI) and Primary Rate Interface (PRI), on the router. This MIB was released as RFC 2127, *ISDN Management Information Base using SMIv2*.

The MODULE-IDENTITY for the ISDN-MIB is isdnMIB, and its top-level OID is 1.3.6.1.2.1.10.20 (iso.org.dod.internet.mgmt.mib-2.transmission.isdnMIB).

MIB Constraint

This MIB is not supported on the Cisco uBR10012 router.

LAN-EMULATION-CLIENT-MIB

The LAN-EMULATION-CLIENT-MIB supplements the ATM-MIB and contains objects to manage the ATM-based LAN emulation clients (LECs) on the router.

The MODULE-IDENTITY for the LAN-EMULATION-CLIENT-MIB is atmfLanEmulation, and its top-level OID is 1.3.6.1.4.1.353.5.3 (iso.org.dod.internet.private.enterprises.atmForum.atmForumNetworkManagement.atmfLanEmulation)

MIB Constraints

This MIB is:

- Supported only on Cisco IOS "-is-" software images for Cisco uBR7100 series and Cisco uBR7200 series routers.
- Not supported on the Cisco uBR10012 router.

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. This MIB is currently in development as an IETF draft, Multicast Source Discovery Protocol MIB (the current version is draft-ietf-msdp-mib-spec-20.txt).

For addition information about this MIB, see the document *MSDP MIB*, at the following URL:

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

The MODULE-IDENTITY for the MSDP-MIB is msdpMIB, and its top-level OID is 1.3.6.1.3.92 (iso.org.dod.internet.experimental.msdpMIB).

MIB Constraints

The MSDP-MIB has the following constraints:

- This MIB is not supported in any Cisco IOS Release 12.1EC software images.
- All other MIB objects—Read-only.

Table 3-41 lists the MSDP-MIB constraints.

Table 3-41 MSDP-MIB Constraints

MIB Object	Notes
msdpRequestsTable	Not supported.
• msdpEstablished	Not supported.

NOTIFICATION-LOG-MIB

The NOTIFICATION-LOG-MIB contains objects that put the SNMP notifications that are sent by the router into a log table for later retrieval or browsing. This MIB was released as RFC 3014, *Notification Log MIB*.

The MODULE-IDENTITY for the NOTIFICATION-LOG-MIB is notificationLogMIB, and its top-level OID is 1.3.6.1.2.1.92 (iso.org.dod.internet.mgmt.mib-2.notificationLogMIB).

MIB Constraints

This MIB is not supported:

- In any Cisco IOS "-is-" software images for Cisco uBR7100 series and Cisco uBR7200 series routers.
- On Cisco uBR10012 routers.

nruCacheSnmpData

Cisco RF Switch Firmware Version 3.80 adds a new MIB object identifier (OID) to control caching on the Cisco CMTS, and the desired state may be set in the AdminState caching flag. To control caching in this manner, use the SNMP object nruCacheSnmpData, which is a read/write integer at OID 1.3.6.1.4.1.6804.2.1.1.9.

The object information for nruCacheSnmpData is as follows:

- Syntax is an integer of 0 or 1.
- Access is read or write.
- The status is mandatory.

Setting the nruCacheSnmpData object with SNMP alters the run-time setting of the cache flag, but does not effect the state of the non-volatile memory (NVRAM) setting. This allows you to override the setting of the cache flag dynamically to verify the state of the settings, if desired.

The state of the NVRAM setting has been added to the **show config** firmware command. The current run-time state has been added to the **show module** firmware command.

SNMP MIB get and set variables can be saved to cache in the AdminState MIB module. The SNMP Cache can be disabled or reenabled using the system-level **set snmp cache** firmware command. The setting for this command is stored in non-volatile memory on the Cisco RF Switch.

Refer to the following document on Cisco.com for additional command information:

- *Release Notes for Cisco RF Switch Firmware, Version 3.80*

  http://www.cisco.com/en/US/docs/cable/rfswitch/ubr3x10/release/notes/rfswrn36.html

MIB Constraints

This object and related functions are supported strictly in Cisco RF Switch Firmware Version 3.80 or later, to be used in conjunction with Cisco IOS Release 12.3BC on the Cisco CMTS.

OLD-CISCO-CHASSIS-MIB

The OLD-CISCO-CHASSIS-MIB describes chassis objects in devices running an older implementation of the Cisco IOS operating system. Although currently supported on the router, the OLD-CISCO-CHASSIS-MIB is being phased out and could become unsupported without prior notice. We recommend that you use the ENTITY-MIB instead of OLD-CISCO-CHASSIS-MIB.

Note The one exception to this recommendation is the chassisId object in this MIB, which can be set using the **snmp-server chassis-id** command. This object provides a convenient location for storing the serial number for the router's chassis, which is typically used to determine the service contract that you have purchased for this router.

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. Although currently supported on the router, the OLD-CISCO-CPU-MIB is being phased out and could become unsupported without prior notice. Therefore, use care if you implement the MIB.

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. Although currently supported on the router, the OLD-CISCO-INTERFACES-MIB is being phased out and could become unsupported without prior notice. Therefore, use care if you implement the MIB.

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. Although currently supported on the router, the OLD-CISCO-IP-MIB is being phased out and could become unsupported without prior notice. Therefore, use care if you implement the MIB.

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 was replaced by the CISCO-MEMORY-POOL-MIB. Therefore, use care if you implement the OLD-CISCO-MEMORY-MIB, which is being phased out and could become unsupported without prior notice.

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. Although currently supported on the router, the OLD-CISCO-SYSTEM-MIB is being phased out and could become unsupported without prior notice. Therefore, use care if you implement the MIB.

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 was replaced by the CISCO-TCP-MIB. Therefore, use care if you implement the OLD-CISCO-TCP-MIB, which is being phased out and could become unsupported without prior notice.

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. Although currently supported on the router, the OLD-CISCO-TS-MIB is being phased out and could become unsupported without prior notice. Therefore, use care if you implement the MIB.

PIM-MIB

The PIM-MIB contains objects to manage Protocol Independent Multicast (PIM) on the router. The MIB was released as RFC 2934, *Protocol Independent Multicast MIB for IPv4*.

Note The MODULE-IDENTITY for the PIM-MIB is pimMIB, and its top-level OID is 1.3.6.1.3.61 (iso.org.dod.internet.experimental.pimMIB).

MIB Constraints

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. This MIB was released as RFC 1213, *Management Information Base for Network Management of TCP/IP-Based Internets: MIB-II*.

The MODULE-IDENTITY for the RFC1213-MIB is mib-2, and its top-level OID is 1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2).

MIB Constraints

Table 3-42 lists the RFC1213-MIB constraints.

Table 3-42 RFC1213-MIB Constraints

MIB Object	Notes
atTable	
• ipInAddrErrors • ipInHdrErrors	These objects can provide inaccurate counts in releases before Cisco IOS Release 12.2(11)BC2.

RFC1231-MIB

The RFC1231-MIB includes objects to manage Token Ring (IEEE 802.5) interfaces. This MIB was released as RFC 1231, *IEEE 802.5 Token Ring MIB,* and has since been superseded by TOKENRING-MIB, which is not supported on Cisco CMTS routers.

MIB Constraint

This MIB was an experimental MIB and is no longer supported on Cisco CMTS platforms, although this MIB might be included in software images.

RFC1253-MIB

The RFC1253-MIB contains objects to manage Version 2 of the Open Shortest Path First (OSPF) protocol. This MIB was released as RFC 1253, *OSPF Version 2 Management Information Base*.

The MODULE-IDENTITY for the RFC1253-MIB is ospf, and its top-level OID is 1.3.6.1.2.1.14 (iso.org.dod.internet.mgmt.mib-2.ospf).

MIB Constraints

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

The MODULE-IDENTITY for the RFC1315-MIB is frame-relay, and its top-level OID is 1.3.6.1.2.1.10.32 (iso.org.dod.internet.mgmt.mib-2.transmission.frame-relay).

MIB Constraints

There are no constraints on this MIB.

RFC1381-MIB

The RFC1381-MIB contains objects to manage the Link Access Procedure, Balanced (LAPB) link layer protocol for X.25 interfaces. This MIB was released as RFC 1381, *SNMP MIB Extension for X.25 LAPB*.

The MODULE-IDENTITY for the RFC1381-MIB is lapb, and its top-level OID is 1.3.6.1.2.1.10.16 (iso.org.dod.internet.mgmt.mib-2.transmission.lapb).

MIB Constraint

This MIB is not supported on the Cisco uBR10012 router.

RFC1382-MIB

The RFC1382-MIB contains objects to manage each Packet Level Entity (PLE) on X.25 interfaces. This MIB was released as RFC 1382, *SNMP MIB Extension for the X.25 Packet Layer*.

The MODULE-IDENTITY for the RFC1382-MIB is x25, and its top-level OID is 1.3.6.1.2.1.10.5 (iso.org.dod.internet.mgmt.mib-2.transmission.x25).

MIB Constraint

This MIB is not supported on the Cisco uBR10012 router.

RFC1406-MIB

The RFC1406-MIB contains objects to manage E1 and DS1 (T1) interfaces. This MIB was released as RFC 1406, *Definitions of Managed Objects for the DS1 and E1 Interface Types*.

The MODULE-IDENTITY for the RFC1595-MIB is ds1, and its top-level OID is 1.3.6.1.2.1.10.18 (iso.org.dod.internet.mgmt.mib-2.transmission.ds1).

MIB Constraints

There are no constraints on this MIB.

RFC1407-MIB

The RFC1407-MIB contains objects to manage E3 and DS3 (T3) interfaces. This MIB was released as RFC 1407, *Definitions of Managed Objects for the DS3/E3 Interface Type*.

The MODULE-IDENTITY for the RFC1595-MIB is ds3, and its top-level OID is 1.3.6.1.2.1.10.30 (iso.org.dod.internet.mgmt.mib-2.transmission.ds3).

MIB Constraints

There are no constraints on this MIB.

RFC1595-MIB

The RFC1595-MIB contains objects to manage Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) interfaces. This MIB was released as RFC 1595, *Definitions of Managed Objects for the SONET/SDH Interface Type* and has since been replaced by the RFC2558-MIB.

The MODULE-IDENTITY for the RFC1595-MIB is sonetMIB, and its top-level OID is 1.3.6.1.2.1.10.39 (iso.org.dod.internet.mgmt.mib-2.transmission.sonetMIB).

MIB Constraint

This MIB is not supported in Cisco IOS Release 12.1EC software images.

RFC2558-MIB

The RFC2558-MIB contains objects to manage Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) interfaces. This MIB was released as RFC 2558, *Definitions of Managed Objects for the SONET/SDH Interface Type*, and it replaces the previous MIB, RFC1595-MIB.

The MODULE-IDENTITY for the RFC2558-MIB is sonetMIB, and its top-level OID is 1.3.6.1.2.1.10.39 (iso.org.dod.internet.mgmt.mib-2.transmission.sonetMIB).

MIB Constraints

This MIB is supported only in Cisco IOS Release 12.1EC and only for Cisco uBR7100 series and Cisco uBR7200 series routers. Cisco IOS Release 12.2BC supports the previous version of this MIB, RFC1595-MIB.

RMON-MIB

The RMON-MIB contains objects to remotely monitor devices in the network. This MIB was released as RFC 1757, *Remote Network Monitoring Management Information Base*.

The MODULE-IDENTITY for the RMON-MIB is rmon, and its top-level OID is 1.3.6.1.2.1.16 (iso.org.dod.internet.mgmt.mib-2.rmon).

MIB Constraints

There are no constraints on this MIB.

RMON2-MIB

The RMON2-MIB contains supplements to RMON-MIB and contains additional objects to remotely monitor devices in the network.

The MODULE-IDENTITY for the RMON2-MIB is rmon2, and its top-level OID is 1.3.6.1.2.1.16 (iso.org.dod.internet.mgmt.mib-2.rmon2).

MIB Constraints

There are no constraints on this MIB.

RS-232-MIB

The RS-232-MIB contains objects to manage RS-232-like (EIA/TIA-232) serial interfaces. This MIB was derived from RFC 1659, *Definitions of Managed Objects for RS-232-like Hardware Devices using SMIv2*.

The MODULE-IDENTITY for the RS-232-MIB is rs232, and its top-level OID is 1.3.6.1.2.1.10.33 (iso.org.dod.internet.mgmt.mib-2.transmission.rs232).

MIB Constraints

There are no constraints on this MIB.

RSVP-MIB

The RSVP-MIB contains objects to manage the Resource Reservation Protocol (RSVP). This MIB was derived from RFC 2206, *RSVP Management Information Base Using SMIv2*.

The MODULE-IDENTITY for the RSVP-MIB is rsvp, and its top-level OID is 1.3.6.1.2.1.51 (iso.org.dod.internet.mgmt.mib-2.rsvp).

MIB Constraints

There are no constraints on this MIB.

SMON-MIB

The SMON-MIB contains objects that supplement the RMON-MIB and the RMON2-MIB to manage the remote monitoring of switched networks. This MIB was derived from RFC 2613, *Remote Network Monitoring MIB Extensions for Switched Networks*.

The MODULE-IDENTITY for the SMON-MIB is switchRMON, and its top-level OID is 1.3.6.1.2.1.16.22 (iso.org.dod.internet.mgmt.mib-2.rmon.switchRMON).

MIB Constraints

There are no constraints on this MIB.

SNMP-COMMUNITY-MIB

The SNMP-COMMUNITY-MIB contains objects to help support coexistence between the different SNMP versions (SNMPv1, SNMPv2c, and SNMPv3). This MIB was released as RFC 2576, *Coexistence Between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework*.

The MODULE-IDENTITY for the SNMP-COMMUNITY-MIB is snmpCommunityMIB, and its top-level OID is 1.3.6.1.6.3.18 (iso.org.dod.internet.snmpv2.snmpModules.snmpCommunityMIB).

MIB Constraints

There are no constraints on this MIB.

SNMP-FRAMEWORK-MIB

The SNMP-FRAMEWORK-MIB contains objects that describe the SNMP management architecture. This MIB was released as RFC 2571, *An Architecture for Describing SNMP Management Frameworks*.

The MODULE-IDENTITY for the SNMP-FRAMEWORK-MIB is snmpFrameworkMIB, and its top-level OID is 1.3.6.1.6.3.10 (iso.org.dod.internet.snmpv2.snmpModules.snmpFrameworkMIB).

MIB Constraints

There are no constraints on this MIB.

SNMP-MPD-MIB

The SNMP-MPD-MIB contains objects from the agent's Message Processing and Dispatching (MPD) server that report on the the total number of packets received by the SNMP engine that were dropped because they referred to an unknown security model, were for an unknown application, or were otherwise invalid. This MIB was released as RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

The MODULE-IDENTITY for the SNMP-MPD-MIB is snmpMPDMIB, and its top-level OID is 1.3.6.1.6.3.11 (iso.org.dod.internet.snmpv2.snmpModules.snmpMPDMIB).

MIB Constraints

There are no constraints on this MIB.

SNMP-NOTIFICATION-MIB

The SNMP-NOTIFICATION-MIB contains objects to manage SNMP v3 notifications. This MIB was released as RFC 2573, *SNMP Applications*.

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.

The MODULE-IDENTITY for the SNMP-NOTIFICATION-MIB is snmpNotificationMIB, and its top-level OID is 1.3.6.1.6.3.13 (iso.org.dod.internet.snmpv2.snmpModules.snmpNotificationMIB).

MIB Constraints

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. This MIB was defined as part of RFC 2573, *SNMP Applications*.

The MODULE-IDENTITY for the SNMP-PROXY-MIB is snmpProxyMIB, and its top-level OID is 1.3.6.1.6.3.14 (iso.org.dod.internet.snmpv2.snmpModules.snmpProxyMIB).

MIB Constraints

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). This MIB was defined as part of RFC 2573, *SNMP Applications*.

The MODULE-IDENTITY for the SNMP-TARGET-MIB is snmpTargetMIB, and its top-level OID is 1.3.6.1.6.3.12 (iso.org.dod.internet.snmpv2.snmpModules.snmpTargetMIB).

MIB Constraints

There are no constraints on this MIB.

SNMP-USM-MIB

The SNMP-USM-MIB contains objects that describe the SNMP User-Based Security Model. This MIB was released as RFC 2574, *User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)*.

The MODULE-IDENTITY for the SNMP-USM-MIB is snmpUsmMIB, and its top-level OID is 1.3.6.1.6.3.15 (iso.org.dod.internet.snmpv2.snmpModules.snmpUsmMIB).

MIB Constraints

There are no constraints on this MIB.

SNMP-VACM-MIB

The SNMP-VACM-MIB contains objects to manage the View-Based Access Control Model (VACM) for SNMP clients and managers. This MIB was released as RFC 2575, *View-Based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

The MODULE-IDENTITY for the SNMP-VACM-MIB is snmpVacmMIB, and its top-level OID is 1.3.6.1.6.3.16 (iso.org.dod.internet.snmpv2.snmpModules.snmpVacmMIB).

MIB Constraints

There are no constraints on this MIB.

SNMPv2-MIB

The SNMPv2-MIB contains objects to manage SNMPv2 entities on the router. This MIB was released as RFC 1907,Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2).

The MODULE-IDENTITY for the SNMPv2-MIB is snmpMIB, and its top-level OIDs are 1.3.6.1.6.3.1 (iso.org.dod.internet.snmpv2.snmpModules.snmpMIB) and 1.3.6.1.2.1.1 (iso.org.dod.internet.mgmt.mib-2.system).

MIB Constraints

There are no constraints on this MIB.

TCP-MIB

The TCP-MIB contains objects to manage the Transmission Control Protocol (TCP) on the router. This MIB was derived from RFC 2012, SNMPv2 Management Information Base for the Transmission Control Protocol Using SMIv2.

The MODULE-IDENTITY for the TCP-MIB is tcpMIB, and its top-level OIDs are 1.3.6.1.2.1.49 (iso.org.dod.internet.mgmt.mib-2.tcpMIB) and 1.3.6.1.2.1.6 (iso.org.dod.internet.mgmt.mib-2.tcp).

MIB Constraints

There are no constraints on this MIB.

UDP-MIB

The UDP-MIB contains objects to manage the User Datagram Protocol (UDP) on the router. This MIB was released as RFC 2013, SNMPv2 Management Information Base for the User Datagram Protocol Using SMIv2.

The MODULE-IDENTITY for the UDP-MIB is udpMIB, and its top-level OIDs are 1.3.6.1.2.1.50 (iso.org.dod.internet.mgmt.mib-2.udpMIB) and 1.3.6.1.2.1.7 (iso.org.dod.internet.mgmt.mib-2.udp).

MIB Constraints

There are no constraints on this MIB.

CHAPTER 4

Monitoring Notifications

This chapter describes the Cisco 7600 Series Router notifications supported by the MIB enhancements feature introduced in Cisco IOS Release 12.3(21)BC. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events. The router also supports other notifications not listed.

This chapter contains the following sections:

- SNMP Notification Overview, page 4-2
- Enabling Notifications, page 4-2
- Cisco SNMP Notifications, page 4-3
  - Functional Notifications, page 4-3
  - Cisco Router Line Card Notifications, page 4-5
  - Flash Card Notifications, page 4-7
  - Link Notifications, page 4-8
  - Packet Forwarding Engine Notifications, page 4-9
  - Configuration Notifications, page 4-10
  - MPLS Service Notifications, page 4-11
  - Interface Trap Descriptions, page 4-11
  - Routing Service Notifications, page 4-15
  - SONET Notifications, page 4-16
  - Chassis Notifications, page 4-17
  - RTT Monitor Notifications, page 4-18
  - Environmental Notifications, page 4-19
  - Redundancy Framework Notifications, page 4-20
  - Cable MIB Notifications, page 4-21

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. Traps are enabled depending on the command snmp-server enable traps.

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, refer the following Cisco documents at:

- *The Traps Sent with SNMP-Server Enabled Traps Configured* guide at: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
- "Configuring SNMP Support" section in *Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2* guide at: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html

Enabling Notifications

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

Using the command-line interface (CLI)—Specify the recipient of the trap message and specify the types of traps sent. For detailed procedures, go to the following URLs:

- *The Traps Sent with SNMP-Server Enabled Traps Configured* guide at: http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a008021de3e.shtml
- *Cisco IOS Software Releases 11.3, SNMP Inform Requests* guide at: http://www.cisco.com/en/US/docs/ios/11_3/feature/guide/snmpinfm.html

- Performing an SNMP SET operation with the **setany** command—To enable or disable MIB notifications, perform an SNMP SET operation on a specific object.
  - To enable the notifications set the object to true(1).
  - To disable the notifications, set the object to false(2).

  For detailed procedures, go to: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/6.x/configuration/guide/snmp.html

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."* appears in the Recommended Action column, there might be instances where an application, such as trouble ticketing, occurs.

Functional Notifications

Table 4-1 lists notifications generated for events that might indicate the failure of the Cisco CMTS uBR router or conditions that might affect the router functionality.

Table 4-1 Environmental and Functional Notifications

Event	Description	Probable Cause	Recommended Action
cefcModuleStatusChange	Indicates that the status of a module has changed. A management application can use this trap to update the status of a module it manages.	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. The trap indicates the entPhysicalIndex of the slot that the line card was inserted in.	A new field replaceable unit like a line card, SIP and SPA modules, fan, port, power supply, or redundant power supply was added.	No action is required; but you can enable this trap through the CLI or by setting cefcMIBEnableStatusNotification to true(1).
cefcFRURemoved	Indicates that a FRU was removed and indicates the entPhysicalIndex of the slot from which the line card was removed.	A field replaceable unit like line cards, SIP and SPA modules, fan, ports, power supply, or redundant power supply was removed.	Replace the field replaceable unit.
chassisAlarmOn	Indicates that a FRU status has changed.	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.

Table 4-1 Environmental and Functional Notifications (continued)

Event	Description	Probable Cause	Recommended Action
	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.	A redundant power supply has been powered on.	No action required.
RAM to CPU Usage	TBD		

Cisco Router 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 CMTS uBR router cards and SPAs.

Table 4-2 Line Card Notifications

Event	Description	Probable Cause	Recommended Action
entConfigChange	An entry for the line card or a shared port adapter is removed from the entPhysicalTable (which causes the value of entLastchangeTime to change).	A line card was removed.	Replace the field replaceable unit.
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 notification reports the most recent measurement seen by the sensor and this notification 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.

Table 4-2 Line Card Notifications (continued)

Event	Description	Probable Cause	Recommended Action
		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.
ceAlarmAsserted	The agent generates this trap when a physical entity asserts an alarm, such as the power entry module 0 failure.	You manually shut down the line card, then you get the line card error or the alarm *Card Stopped Responding OIR* occurs.	Check the entPhysicalDescr type and take the corresponding action; because there are many types of asserted alarms.
ceAlarmCleared	The agent generates this trap when a physical entity clears a previously asserted alarm or when the core or inlet temperature crosses a threshold, such as inlet critical temperature limit.	The agent generates this trap when: • a physical entity clears a previously asserted alarm • a line card is installed in a slot and the alarm *Active Card Removed OIR* is cleared.	

Notes:

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

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

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

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

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

RAM to CPU Usage	TBD		

Flash Card Notifications

Table 4-3 lists CISCO-FLASH-MIB notifications generated by Cisco CMTS uBR router 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 when a removable flash card is inserted in the router.	To determine which flash card was inserted, use the ciscoFlashDeviceIndex to check the ciscoFlashDeviceTable.
entConfigChange	This is generated every time a conceptual row is created, modified, or deleted in any of the following tables: • entPhysicalTable • entLogicalTable • entLPMappingTable • entAliasMappingTable • entPhysicalContainsTabl That means a new device (flash or any card) is added or removed from the router. And the entLastChangeTime is the sysUpTime at the time a flash card is added or deleted.	Status change occurred when a flash card was added or removed.	To determine which flash card was removed from the router, use the ciscoFlashDeviceIndex to check the ciscoFlashDeviceTable.
ciscoFlashCopyCompletionTrap **ciscoFlashPartitioningCompletionTrap** **ciscoFlashMiscOpCompletionTrap**	Indicates that a flash operation has occurred.	Sent when the following flash operations occur: • copy operation finishes • partitioning operation finishes • miscellaneous flash card operation finishes	Enable this trap through the CLI or setting the corresponding flash object to true(1).

Link 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 current state. Value is down(2). • Indicates that the wideband downstream ports on the SPA are in a down state.	An internal software error might have occurred.	To see if link traps are enabled or disabled on an interface, check ifLinkUpDownTrapEnable (IF-MIB) for the interface. To enable link traps, set ifLinkUpDownTrapEnable to enabled(1). Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**.
linkUp	• Indicates that a link is about to enter the Up state and the ifOperStatus object shows the link's current status. • Indicates that the wideband downstream ports on the SPA are in a up state.	The port manager reactivated a port in the link-down state during a switchover.	To see if link traps are enabled or disabled on an interface, check ifLinkUpDownTrapEnable (IF-MIB) for the interface. To enable link traps, set ifLinkUpDownTrapEnable to enabled(1). Enable the IETF (RFC 2233) format of link traps by issuing the CLI command **snmp-server trap link ietf**.

Packet Forwarding Engine Notifications

Table 4-5 lists notifications generated by the router for Packet Forwarding Engine (PFE) events on the Cisco uBR10012 router. The Cisco uBR10012, the PFE is the parallel express forwarding network processor (PXF), which is part of the performance routing engine (PRE).

Table 4-5 Packet Forwarding Engine Notifications

Event	Description	Probable Cause	Recommended Action
cePfeHistThldEvent Objects: • cePfeHistEntPhysIndex, • cePfeHistType, • cePfeHistThld, • cePfeHistValue	Indicates that the configured threshold is crossed. The threshold value and the type are found from the cePfeHistType and cePfeHistThld. And the event type can be any of the enumerations of the HistEventType.	A threshold event has occurred and the cePfeHistNotifiesEnable is set to notify(3) or logAndNotify(4).	After generation this notification, another notification is not sent out until the sample value falls below the threshold value.
HistEventType			
• thldUtilizationEvent	Generated if the cePfePerfCurrentUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThldUtilization		
• thldEfficiencyEvent	Generated if the cePfePerfCurrentEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThldEfficiency.		
• thld1MinUtilizationEvent	Generated if the cePfePerfCurrent1MinUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThld1MinUtilization.		
• thld1MinEfficiencyEvent	Generated if the cePfePerfCurrent1MinEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThld1MinEfficiency.		

Table 4-5 Packet Forwarding Engine Notifications (continued)

Event	Description	Probable Cause	Recommended Action
• thld5MinUtilizationEvent	Generated if the cePfePerfCurrent5MinUtilization, at the time of sampling, becomes greater than or equal to the cePfePerfThld5MinUtilization.		
• thld5MinEfficiencyEvent	Generated if the cePfePerfCurrent5MinEfficiency, at the time of sampling, becomes less than or equal to the cePfePerfThld5MinEfficiency.		
cePfeHistRestartEvent	Indicates a PFE restart occurred.	The PFE processor restarted	Enable this trap using the CLI **snmp-server** command or by setting cePfeHistNotifiesEnable to notify(3) or logAndNotify(4)

Configuration Notifications

Table 4-6 lists notifications generated by the CMTS router for events related to system configuration.

Table 4-6 CMTS Configuration Notifications

Event	Description	Probable Cause	Recommended Action
ccCopyCompletion • ccCopyServerAddress • ccCopyFileName • ccCopyState • ccCopyTimeStarted • ccCopyTimeCompleted • ccCopyFailCause	A ccCopyCompletion trap is sent when a config-copy request is completed. The ccCopyFailCause is not instantiated, and hence not included in a trap, when the ccCopyState is successful.	Sent when the CMTS router finishes copying a configuration file to or from another location.	Enable this trap by setting ccCopyNotificationOnCompletion to true(1).
ciscoConfigManEvent	The current configuration changed.	Sent when the running configuration changes.	No action required.

MPLS Service Notifications

Table 4-7 lists service notifications generated by the CMTS router to indicate conditions for services.

Table 4-7 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. May be caused by an administrative or operational status check of the tunnel.	No action is required. Enable this trap through the CLI or by setting mplsTunnelTrapEnable to true(1)>
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. May be caused by an administrative or operational status check of the tunnel.	
mplsTunnelRerouted	Indicates that the signalling path for an MPLS traffic engineering tunnel changed.	A tunnel was rerouted or reoptimized.	If you use the actual path, then write the new path to mplsTunnelRerouted after the notification is issued.

Interface Trap Descriptions

To be provided

Admin Status of Interface Up/Down

Admin Status of Subinterface Up/Down

Table 4-8 Interface and Subinterface Traps

Event	Trap and Trap Objects	Notes
Admin Status of Interface Up/Down	-MIB	
	•	
	-MIB	
	•	
	-MIB	
	•	
Admin Status of Subinterface Up/Down	-MIB	
	•	
	-MIB	
	•	

Routing Protocol Notifications

Table 4-9 lists notifications generated by the Cisco CMTS uBR router to indicate error conditions for routing protocols.

Table 4-9 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> [threshold] [warning-only]**
oamLoopbackPingCompletionTrap	Indicates a loopback test.	Sent when an OAM loopback test completes.	Enable this trap through the CLI or by setting oamLoopbackPingTrapOnCompletion to true(1).
cPppoeSystemSessionThresholdTrap	Indicates that the PPPoE system session exceeded a threshold.	Sent when the number of active PPPoE sessions exceeds the value of cPppoeSystemThresholdSessions.	Enable this trap through the CLI.
cPppoeVcSessionThresholdTrap	Indicates that the PPPoE VC session exceeded a threshold.	Sent when the number of active PPPoE sessions on the VC exceeds the value of cPppoeVcThresholdSessions.	Enable this trap through the CLI.

Interface Trap Descriptions

To be provided

Admin Status of Interface Up/Down

Admin Status of Subinterface Up/Down

Table 4-10 Interface and Subinterface Traps

Event	Trap and Trap Objects	Notes
Admin Status of Interface Up/Down	-MIB	
	•	
	-MIB	
	•	
	-MIB	
	•	
Admin Status of Subinterface Up/Down	-MIB	
	•	
	-MIB	
	•	

Routing Service Notifications

Table 4-11 lists notifications generated by the Cisco CMTS uBR router to indicate error conditions for routing services.

Table 4-11 Routing Protocol Notifications

Event	Description	Probable Cause	Recommended Action
casServerStateChange	The casState object changes status. 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. The number of minutes casState remains dead(2) is specified by the radius-server deadtime minutes command. For example, if server deadtime is 5 minutes and an AAA request fails, a trap is generated with casState set to dead(2). Five minutes later, another trap is generated with casState set to up(1) even though the server may still be down.	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: • up(1)—Send requests to the server. • dead(2)—Do not send requests to the server. Send requests to the next available server instead.	Enable this trap by setting casServerStateChangeEnable to true(1).
ciscoSsgRadiusClientReboot	Sent when the Service Selection Gateway (SSG) detects that a RADIUS client has rebooted. (SSG uses RADIUS servers to authenticate subscribers.)	A RADIUS client has rebooted.	Enable this trap by setting ssgCfgRadiusClientRebootNotification to true(1).

SONET Notifications

Table 4-12 lists alarm notifications generated by the router for SONET events.

Table 4-12 SONET Notifications

Event	Description	Probable Cause	Recommended Action
ceAssertAlam **ceClearAlarm**	These notifications indicate error conditions on a SONET circuit and the status of SONET layers. Note that not all SONET and Packet over SONET (POS) line cards generate all of the traps.	Sent when one of the following alarm status has changed. See footnote below.	Check out the AlarmType and ceAlarmHistSeverity values.
Paths, for example a Path Alarm Indication Signal Line, for example a Line Remove Failure Indication Section, for example a Section Loss of Frame Failure Clock problems, for example a Far End Clock Out of Range Signal, for example a Out of Frame Failure Near End/Far End, for example a Far End Alarm Indication Signal Thresholds, for example a Threshold Cross Alarm-B1			

Chassis Notifications

Table 4-13 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 CMTS router.

Table 4-13 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 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.	Replace module.
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 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.	No action required.

RTT Monitor Notifications

Table 4-14 lists CISCO-RTTMON-MIB notifications that can occur during round-trip time (RTT) monitoring.

Table 4-14 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. Note that this is a connection to a target not to a hop in the path to the target.	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 during an RTT probe.	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. No action is required if rttMonCtrlOperTimeoutOccurred is false.
rttMonThresholdNotification	Threshold violation occurred during an RTT probe.	Indicates that the previous violation has subsided for a subsequent RTT operation. which results in rttMonCtrlOperOverThresholdOccurred changing value.	Check for the end-to-end connectivity if rttMonCtrlOperOverThresholdOccurred in the notification is true otherwise no action required.

Environmental Notifications

Table 4-15 lists CISCO-ENVMON-MIB notifications generated for events that might indicate the failure of the Cisco CMTS uBR router or conditions that might affect the router's functionality.

Table 4-15 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). 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 system critical alarms like facility-alarm-intake-temperature. Enable this trap through the following CLI command **snmp-server-enable traps envmon shutdown** or by setting the ciscoEnvMonEnableShutdownNotification to true(1).
ciscoEnvMonFanNotification	Fan status. A ciscoEnvMonFanNotification is sent if the system detects a fan failure or an empty tray.	One or more fans in the system fan tray have failed, or the fan tray is missing. Although this is a minor alarm, system components could overheat and be shut down.	Replace the system fan tray. Enable this trap using the CLI *snmp-server-enable traps envmon fan* command or by setting ciscoEnvMonEnableFanNotification to true (1).
ciscoEnvMonRedundantSupplyNotification	Power supply status. 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. Enable this trap using the CLI **snmp-server enable traps envmon supply** command or by setting ciscoEnvMonEnableRedundantSupplyNotification to true (1).

Table 4-15 Environmental Notifications (continued)

Event	Description	Probable Cause	Recommended Action
ciscoEnvMonTempStatusChangeNotif	Temperature status. The core or inlet temperature is outside its normal range, when ciscoEnvMonState is at the Warning or Critical state. 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. Enable this trap using the CLI **snmp-server enable traps envmon temperature** command or by setting ciscoEnvMonEnableTemperatureNotification to true (1).

* 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.

Redundancy Framework Notifications

Table 4-16 lists CISCO-RF-MIB notifications that can occur in a redundant system. There are two types of notifications:

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

Table 4-16 Redundancy Framework Notifications

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

Cable MIB Notifications

Table 4-17 lists the notifications that occur in the following supported MIBs:

- DOCS-CABLE-DEVICE-TRAP-MIB
- CISCO-DOCS-REMOTE-QUERY-MIB
- CISCO-CABLE-METERING-MIB
- CISCO-DOCS-EXT-MIB

Table 4-17 CABLE MIB Notifications

MIB and Event	Description	Probable Cause	Recommended Action
DOCS-CABLE-DEVICE-TRAP-MIB			
• docsDevCmtsInitRegReqFailTrap	Indicates that a registration request failed. The failure was detected on the CMTS side.	A registration request failed during the CM initialization process.	Correct the registration request failure.
• docsDevCmtsInitRegRspFailTrap	Indicates a registration response failed. The failure was detected on the CMTS side.	A registration response failed during the CM initialization process.	Correct the registration response failures.
• docsDevCmtsInitRegAckFailTrap	Indicates a registration acknowledgement failed. The failure was detected on the CMTS side.	A registration acknowledgement failed during the CM initialization process.	Correct the registration acknowledgement failures.

Table 4-17 CABLE MIB Notifications (continued)

MIB and Event	Description	Probable Cause	Recommended Action
• docsDevCmtsDynServReqFailTrap	Indicates a dynamic service request failed. The failure was detected on the CMTS side.	A dynamic service request failed during the dynamic services process.	Correct the dynamic service request failures.
• docsDevCmtsDynServRspFailTrap	Indicates a dynamic service response failed. The failure was detected on the CMTS side.	A dynamic service response failed during the dynamic services process.	Correct the dynamic service response failures.
• docsDevCmtsDynServAckFailTrap	Indicates a dynamic service acknowledgement failed. The failure was detected on the CMTS side.	A dynamic service acknowledgement failed during the dynamic services process.	Correct the dynamic service acknowledgement failures.
• docsDevCmtsBpiInitTrap	Indicates a BPI initialization attempt failed. The failure was detected on the CMTS side.	A BPI initialization attempt failed during the CM registration process.	Correct the BPI initialization attempt failures.
• docsDevCmtsBPKMTrap	Indicates a BPKM operation failed. The failure was detected on the CMTS side.	A BPKM operation failed.	Correct the BPKM operation failures.
• docsDevCmtsDynamicSATrapTrap	Indicates a dynamic security association operation failed. The failure was detected on the CMTS side.	A dynamic security association operation failed.	Correct the dynamic security association operation failures.
• docsDevCmtsDCCReqFailTrap	A dynamic channel change request failed. The failure was detected on the CMTS side.	A dynamic channel change request failed during the dynamic channel change process	Correct the dynamic channel change request failures.
• docsDevCmtsDCCRspFailTrap	Indicates a dynamic channel change response failed. The failure was detected on the CMTS side.	A dynamic channel change response failed during the dynamic channel change process.	Correct the dynamic channel change response failures.
• docsDevCmtsDCCAckFailTrap	A dynamic channel change acknowledgement failed. The failure was detected on the CMTS side.	A dynamic channel change acknowledgement failed during the dynamic channel change process.	Correct the dynamic channel change acknowledgement failures.

Table 4-17 CABLE MIB Notifications (continued)

MIB and Event	Description	Probable Cause	Recommended Action
1 The following traps can be enabled using the CLI **snmp-server enable trap docsis-cmts** command. bpi—Enable BPI init fail trap bpkm—Enable BPKM fail trap dccack—Enable dynamic channel change acknowledgement fail trap dccreq—Enable dynamic channel change request fail trap dccrsp—Enable dynamic channel change response fail trap dsack—Enable dynamic service acknowledgement fail trap dsreq—Enable dynamic service request fail trap dsrsp—Enable dynamic service response fail trap dynsa—Enable Dynamic SA fail trap regack—Enable registration acknowledgement fail trap regreq—Enable registration request fail trap regrsp—Enable registration response fail trap 2 The following traps can be enabled by setting the bit value in docsDevCmtsTrapControl: cmtsInitRegReqFailTrap(0) cmtsInitRegRspFailTrap(1) cmtsInitRegAckFailTrap(2) cmtsDynServReqFailTrap(3) cmtsDynServRspFailTrap(4) cmtsDynServAckFailTrap(5) cmtsBpiInitTrap(6) cmtsBPKMTrap(7) cmtsDynamicSATrap(8) cmtsDCCReqFailTrap(9) cmtsDCCRspFailTrap(10) cmtsDCCAckFailTrap(11)			
DOCS-REMOTE-QUERY-MIB			
• cdrqCmtsCmRQDoneNotification	Indicates the CMTS CM poller finished polling for the current cycle.		
• cdrqCmtsCmPollerStartTime	Indicates the time when the polling cycle started.	CMTS CM poller started polling.	No action required
• cdrqCmtsCmPollerStopTime	Indicates the time when the polling cycle finished.	CMTS CM poller finished polling.	No action required
CISCO-CABLE-METERING-MIB			
ccmtrCollectionNotification	Indicates if the metering record file was created successfully or not and if streaming the file to the collection server was successful or not.	The receipt of this notification is an indication to the collection server that the file can be accessed through ftp or any file transfer protocol in the case of local storage.	Enable this trap by setting ccmtrMeteringNotifEnable to true(1)

Table 4-17 CABLE MIB Notifications (continued)

MIB and Event	Description	Probable Cause	Recommended Action
• ccmtrCollectionStatus, • ccmtrCollectionDestination, • ccmtrCollectionTimestamp	Indicates the success or failure of the export. Indicates the destination of the export in both the success and failure scenarios. Indicates the timestamp of the export in both the success and failure scenarios.		
cdxCmtsCmDMICLockNotification	Indicates a failure relating to DMIC.	Sent whenever a modem is locked because it failed the Dynamic Message Integrity Check (DMIC).	
ccsSpecMgmtNotification	Describes a change in status for cable hopping, modulation profile, or channel width.	Cable upstream runtime frequency (hopping), profile, or channel width status changed. See footnote below.	Use the cable upstream threshold command to change these values The CNR threshold for the secondary modulation profile defaults to 15 dB. The correctable FEC error threshold defaults to 1 percent of total packets received, and the invalid FEC error threshold defaults to 1 percent of total packets received.

1. In the case of frequency hopping, ccsUpSpecMgmtHopCondition would indicate whether SNR or modemOffline that caused the hopping.
2. Frequency hopping is based on the carrier-to-noise ratio (CNR) and the correctable FEC error and uncorrectable FEC error values. A channel will frequency hop if the CNR falls below the configurable threshold AND either the correctable or uncorrectable FEC error values exceed the configurable threshold values.
3. Channel width may be too small.

APPENDIX A

Using Cisco CMTS MIBs

This chapter describes the objects and MIBs that are needed to use Simple Network Management Protocol (SNMP) requests to perform the following tasks on a Cisco CMTS universal broadband router.

- Tips and Guidelines, page A-1
- Obtaining Basic Information About the Router, page A-3
- Managing Physical Components, page A-4
- Generating SNMP Traps, page A-12
- Monitoring SYSLOG Messages, page A-15
- Displaying Information About Cable Modems, page A-17
- Monitoring Spectrum Management, page A-20
- Using Flap Lists, page A-29
- Using Subscriber Traffic Management, page A-34
- Usage-Based Billing, page A-36
- Identifying Cisco Unique Device Identifiers, page A-41
- DOCS-DSG-IF-MIB Validation Requirements, page A-41

Tips and Guidelines

When using SNMP to manage the Cisco CMTS router, be aware of the following points.

IF-MIB Caching

In Cisco IOS Release 12.2(15)BC1c and later releases, the Cisco CMTS routers implemented a cache to allow continuous polling of the ifTable interface counters, without creating spikes in the CPU usage. An SNMP request for these counters returns the values that were last stored in the counter cache memory, instead of returning the current run-time value of these counters. This improves performance, because it means the Cisco IOS software does not have to poll each line card to obtain these counters when an SNMP request is made.

The ifTable counter cache is updated approximately every 10 seconds, which means that if you read the ifTable interface counters more quickly than every 10 seconds, the SNMP request might not return new values. The run-time counters do continue to increment, however, to account for the actual traffic occurring on the interfaces, and another SNMP request in 10 seconds does show the new values.

SNMP-Based and CLI-Based Counters

The SNMP specifications do not allow most SNMP-based counters to be cleared, except at system initialization. Instead, during normal operations the counters continue incrementing until they reach their maximum value, at which point they wrap around to zero and continue incrementing again.

This behavior requires the following considerations when managing the router using SNMP commands:

- 32-bit counters—A 32-bit counter wraps around to zero after reaching approximately 4.2 billion. On a busy router, this means that byte and packet counters could wrap around after only a few days. To ensure that you are maintaining the correct counts for packets and other objects, regularly poll the desired counters and always save the previous values. Subtract the previous value from the current value, and if the difference between the two counters becomes negative, it indicates that the counters have wrapped.

  To accurately total the counters over a period of several weeks or months, you might also need to keep track of the number of times that the counter wraps during this time period. You should poll the counters often enough so that they do not wrap around to zero more than once without being detected.

Tip Some SNMPv3 MIBs are beginning to include 64-bit counters, as well as 32-bit counters, for many of the same objects. If given a choice, use the 64-bit counters, because they typically will not wrap around to zero for months or years, if ever.

- Counting from a specified event or time period—SNMP-based counters begin incrementing from zero when the router is powered on, and continue incrementing until they wrap. To track the number of packets or other objects from a particular event, you must save the value of the counters at the time of the event. Then when you want to obtain a new packet count, compare the current value of the counters with the saved value.
- Comparison with command-line interpreter (CLI) values—Many **show** commands have a corresponding **clear** command that resets the counters to zero. The **clear** command, however, affects only the counters that are displayed by the CLI, not the SNMP-based counters. In addition, many CLI-based counters automatically reset whenever a certain function, such as resetting an interface, is performed. This means that the counters displayed using CLI commands are not usually the same as the counters displayed by SNMP commands. Be aware of these differences when comparing the CLI-based and SNMP-based counters.

Redundant PRE Modules on the Cisco uBR10012 Router

On a Cisco uBR10012 router running Cisco IOS Release 12.2BC, SNMP configuration commands are not synchronized to the standby redundant Performance Routing Engine (PRE) module, as is the case with CLI commands. This means that any configuration that is done with SNMP commands is not active when a switchover occurs and the standby PRE module becomes active. When the router switches back to the original PRE module, the original configuration is restored.

For critical configurations, use CLI commands and save them to the startup-config to ensure that they are active during any switchovers.

Obtaining Basic Information About the Router

Basic information about the Cisco CMTS router can be obtained from objects in the following MIBs:

- OLD-CISCO-CHASSIS-MIB, page A-3
- SNMPv2-MIB, page A-3
- ENTITY-MIB, page A-4

OLD-CISCO-CHASSIS-MIB

The following object in the OLD-CISCO-CHASSIS-MIB provides a convenient location to store the chassis serial number for the router, so that it can be easily retrieved when calling Cisco Technical Support:

- chassisId—Provides the serial number or ID number for the chassis, as defined by the **snmp-server chassis-id** command, which is typically used to identify the service contract and levels of service that you have purchased from Cisco Technical Support. This object defaults to the empty string, so you must use the **snmp-server chassis-id** command to set the value of this object before you can retrieve it.

```
csh% getmany -v2c 10.10.11.12 public chassisId

chassisId.0 = TBA06500113
```

SNMPv2-MIB

The following objects in the SNMPv2-MIB provide basic information about the router, its software, and other run-time information:

- sysDescr—Provides an overall description of the router, including its model number and the version of Cisco IOS software that it is running. For example:

```
csh% getmany -v2c 10.10.11.12 public sysDescr

sysDescr.0 = Cisco Internetwork Operating System Software
IOS (tm) 10000 Software (UBR10K-K8P6-M), Released Version 12.2(15)BC1
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 23-Jan-04 23:56 by atifg
```

- sysObjectID—Provides the specific model number, as it is defined in the CISCO-PRODUCTS-MIB. For example:

```
csh% getmany -v2c 10.10.11.12 public sysObjectId

sysObjectID.0 = ciscoProducts.ciscoUBR10012
```

- sysName—Provides the host name for the router, as assigned by the **hostname** command. For example:

```
csh% getmany -v2c 10.10.11.12 public sysName

sysName.0 = UBR10012-Router
```

- sysUpTime—Provides the time, in hundredths of a second, since the router was last initialized. For example:

```
csh% getmany -v2c 10.10.11.12 public sysUpTime
```

```
sysUpTime.0 = 138389875
```

- sysContact—Provides the name, phone number, or other identifying information for the person or department responsible for this router, as it was entered using the **snmp-server contact** command. For example:

```
csh% getmany -v2c 10.10.11.12 public sysContact

sysContact.0 = IT Support at 408-555-1212 or epage it-support
```

- sysLocation—Provides a description of the router's location, as it was entered using the **snmp-server location** command. For example:

```
csh% getmany -v2c 10.10.11.12 public sysLocation
```

ENTITY-MIB

The following objects in the ENTITY-MIB provide basic information about the router's hardware:

- entPhysicalDescr—Provides a description of each hardware component in the router. For example, the following is a typical description for the Cisco uBR7246VXR chassis:

```
csh% getnext -v2c 10.10.11.12 public entPhysicalDescr

entPhysicalDescr.1 = uBR7246VXR chassis, Hw Serial#: 65100, Hw Revision: A
```

- entPhysicalHardwareRev—Provides the hardware revision of each component, if present and supported for that particular component. For example:

```
csh% getnext -v2c 10.10.11.12 public entPhysicalHardwareRev

entPhysicalHardwareRev.1 = 1.1
```

- entPhysicalSerialNum—Provides the serial number for each component, if present and supported for that particular component. For example:

```
csh% getnext -v2c 10.10.11.12 public entPhysicalSerialNum

entPhysicalSerialNum.1 = TBC06481339
```

- entPhysicalModelName—Provides the model name for each component, if present and supported for that particular component. For example:

```
csh% getnext -v2c 10.10.11.12 public entPhysicalModelName

entPhysicalModelName.1 = uBR7246VXR
```

Tip Also see the next section for more information about the ENTITY-MIB and how to use it.

Managing Physical Components

The Cisco CMTS router supports a number of MIBs for the management of the router's physical components. These MIBs provide the following functions:

- 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)
- Maps physical ports to their respective interfaces
- Provides asset information for asset tagging
- Provides firmware and software information for chassis components

See the following sections for a description of each MIB, as well as instructions on how to use the MIBs to track the components in the router:

- ENTITY-MIB, page A-5
- Cisco-Specific MIBS, page A-6
- Performing Inventory Management, page A-6

Tip To retrieve the chassis serial number for the router, retrieve the chassisId object from the OLD-CISCO-CHASSIS-MIB. This object defaults to the empty string, so you must use the **snmp-server chassis-id** command to set the value of this object before you can retrieve it.

ENTITY-MIB

The Cisco CMTS router uses the ENTITY-MIB, which is defined as the standard RFC 2737, to manage its physical components, which are known as entities. An entity could be a card, a port on a card, a major subsystem on a card, a slot in the chassis, a field-replaceable unit (FRU), or any other equipment that is installed in the router.

The ENTITY-MIB defines a set of objects that uniquely identify each entity in the router, using a hierarchical containment tree that shows how each entity relates to each other. Other MIBs can then use the objects defined by the ENTITY-MIB to provide additional information about each entity.

The following are the most important objects in the ENTITY-MIB for the management of physical entities on the router:

- entPhysicalTable—Describes each physical component (entity) in the router. The table contains a row entry for the top-most entity (the chassis) and then for each entity in the chassis. Each entry provides the name and description of the entry, its type and vendor, and a description of how the entity fits into the containment tree.
- entPhysicalIndex—Uniquely identifies each entry. This value is guaranteed to be unique across all equipment in this chassis and across all MIBs, allowing you to correlate the data from several MIBs for any particular entity.
- entAliasMappingTable—Maps each physical port's entPhysicalIndex value to the corresponding ifIndex value in the ifTable in the IF-MIB. This provides a quick way of identifying a particular port with a particular interface.

  In Cisco IOS Release 12.2(15)BC2 and later releases, the entAliasMappingTable also shows the mapping of physical upstream connectors to logical upstream interface when virtual interfaces are configured on the Cisco uBR-MC5X20S and Cisco uBR-MC5X20U cable interface line cards. This support also changed the parent-child relationships of cable interface line cards and their ports. For more information, see the "Changes to Support Virtual Interfaces" section on page 3-76.
- entPhysicalContainsTable—For each physical entity, lists the entPhysicalIndex value for any child objects of the entity. This provides an easy way of creating the container tree for the router, which shows the relationship between physical entities in the chassis.

  Typically, the container tree is organized as follows:

- The chassis is the topmost level and contains the processor card and chassis slots.
- Chassis slots contain the individual line cards and I/O controller (if installed).
- Line cards contain ports (interfaces).
- Cable interface line cards contain downstream ports (known as cable line card, CLC). In Cisco IOS Release 12.2(15)BC1 and earlier releases, each downstream port then contains the upstream ports that are associated with it. In Cisco IOS Release 12.2(15)BC2 and later releases, the downstream ports and upstream are all children of the cable interface line card.

Cisco-Specific MIBS

In addition to the ENTITY-MIB, the Cisco CMTS router uses the following MIBs to provide additional information about the physical components that are installed in the router:

- 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, and manufacturing assembly number, as well as 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.

Performing Inventory Management

The ENTITY-MIB provides all of the information needed to collect an inventory of the physical components in the router. The following procedure illustrates one way this can be done, using a Cisco uBR7246VXR router. In this example, the router contains the following cards:

- I/O Slot: Dual Fast Ethernet I/O Controller (FastEthernet0/0 and FastEthernet0/1)
- Slot 1: Fast Ethernet Line Card (FastEthernet1/0 and FastEthernet1/1)
- Slot 4: Cisco uBR-MC28U
- Slot 6: Cisco uBR-MC16E

To collect and organize the information in the ENTITY-MIB, use the following procedure.

Step 1 Collect the list of physical entities by displaying all of the entPhysicalDescr objects. For example:

```
entPhysicalDescr.1 = uBR7246VXR chassis, Hw
Serial#: 65100, Hw Revision: A
entPhysicalDescr.2 = NPE 400 Card
entPhysicalDescr.3 = Chassis Slot
entPhysicalDescr.4 = I/O Dual Fast Ethernet
Controller
entPhysicalDescr.5 = i82543 (Livengood)
entPhysicalDescr.6 = i82543 (Livengood)
entPhysicalDescr.7 = Chassis Slot
entPhysicalDescr.8 = Dual Port Fast
Ethernet (RJ45)
entPhysicalDescr.9 = i82543 (Livengood)
entPhysicalDescr.10 = i82543 (Livengood)
entPhysicalDescr.11 = Chassis Slot
entPhysicalDescr.12 = Chassis Slot
entPhysicalDescr.13 = Chassis Slot
entPhysicalDescr.14 = MC28U_F_connector
entPhysicalDescr.15 = UBR7200 CLC
entPhysicalDescr.16 = UBR7200 CLC
entPhysicalDescr.17 = BCM3138 PHY
entPhysicalDescr.18 = BCM3138 PHY
entPhysicalDescr.19 = BCM3138 PHY
entPhysicalDescr.20 = BCM3138 PHY
entPhysicalDescr.21 = BCM3034 PHY
entPhysicalDescr.22 = BCM3138 PHY
entPhysicalDescr.23 = BCM3138 PHY
entPhysicalDescr.24 = BCM3138 PHY
entPhysicalDescr.25 = BCM3138 PHY
entPhysicalDescr.26 = BCM3034 PHY
entPhysicalDescr.27 = Chassis Slot
entPhysicalDescr.28 = Chassis Slot
entPhysicalDescr.29 = MC16E
entPhysicalDescr.30 = BCM3210 ASIC
entPhysicalDescr.31 = BCM3137 PHY
entPhysicalDescr.32 = BCM3137 PHY
entPhysicalDescr.33 = BCM3137 PHY
entPhysicalDescr.34 = BCM3137 PHY
entPhysicalDescr.35 = BCM3137 PHY
entPhysicalDescr.36 = BCM3137 PHY
entPhysicalDescr.37 = BCM3033 PHY
```

Step 2 Obtain additional information about each entPhysicalDescr object by collecting the entPhysicalVendorType, entPhysicalName, and entPhysicalClass objects. Use the index value to match the objects with their corresponding entPhysicalDescr object. Table A-1 shows typical descriptions for the objects used in this example.

Table A-1 Sample entPhysicalDescr Objects and Descriptions

Index #	entPhysicalDescr[1]	entPhysicalVendorType	entPhysicalName	entPhysicalClass
1	uBR7246VXR chassis, Hw Serial#: 012345, Hw Revision: A	cevChassisUbr7246Vxr		chassis(3)
2	NPE 400 Card	cevCpu7200Npe400		module(9)
3	Chassis Slot	cevContainerSlot		container(5)
4	I/O Dual Fast Ethernet Controller	cevC7xxxIo2FE		module(9)
5	i82543 (Livengood)	cevPortFEIP	FastEthernet0/0	port(10)
6	i82543 (Livengood)	cevPortFEIP	FastEthernet0/1	port(10)
7	Chassis Slot	cevContainerSlot		container(5)
8	Dual Port Fast Ethernet (RJ45)	cevPa2feTxI82543		module(9)
9	i82543 (Livengood)	cevPortFEIP	FastEthernet1/0	port(10)
10	i82543 (Livengood)	cevPortFEIP	FastEthernet1/1	port(10)
11	Chassis Slot	cevContainerSlot		container(5)
12	Chassis Slot	cevContainerSlot		container(5)
13	Chassis Slot	cevContainerSlot		container(5)
14	MC28U_F_connector	cevModuleUbrType		module(9)
15	UBR7200 CLC	cevPortRfMac	Cable4/0	port(10)
16	UBR7200 CLC	cevPortRfMac	Cable4/1	port(10)
17	BCM3138 PHY	cevPortRfUs	Cable4/0-upstream0	port(10)

Table A-1 Sample entPhysicalDescr Objects and Descriptions (continued)

Index #	entPhysicalDescr[1]	entPhysicalVendorType	entPhysicalName	entPhysicalClass
18	BCM3138 PHY	cevPortRfUs	Cable4/0-upstream1	port(10)
19	BCM3138 PHY	cevPortRfUs	Cable4/0-upstream2	port(10)
20	BCM3138 PHY	cevPortRfUs	Cable4/0-upstream3	port(10)
21	BCM3034 PHY	cevPortRfDs	Cable4/0-downstream	port(10)
22	BCM3138 PHY	cevPortRfUs	Cable4/1-upstream0	port(10)
23	BCM3138 PHY	cevPortRfUs	Cable4/1-upstream1	port(10)
24	BCM3138 PHY	cevPortRfUs	Cable4/1-upstream2	port(10)
25	BCM3138 PHY	cevPortRfUs	Cable4/1-upstream3	port(10)
26	BCM3034 PHY	cevPortRfDs	Cable4/1-downstream	port(10)
27	Chassis Slot	cevContainerSlot		container(5)
28	Chassis Slot	cevContainerSlot		container(5)
29	MC16E	cevUbrMc16e		module(9)
30	BCM3210 ASIC	cevPortRfMac	Cable6/0	port(10)
31	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream0	port(10)
32	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream1	port(10)
33	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream2	port(10)
34	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream3	port(10)
35	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream4	port(10)
36	BCM3137 PHY	cevPortRfUs	Cable6/0-upstream5	port(10)
37	BCM3033 PHY	cevPortRfDs	Cable6/0-downstream	port(10)

1. Interfaces are typically identified by the chipset that is being used for the interface's connectors. On cable interfaces, upstreams are further identified by the chipsets that are providing the PHY-layer connectivity.

Step 3 To create the containment tree for the router, collect the EntPhysicalContainedIn object for each entPhysicalDescr object. The value in EntPhysicalContainedIn is the index number for the parent (or "container") for the corresponding entPhysicalDescr device.

The following shows the entPhysicalContainedIn values for the objects being used in this example:

```
entPhysicalContainedIn.1 = 0
entPhysicalContainedIn.2 = 1
entPhysicalContainedIn.3 = 1
entPhysicalContainedIn.4 = 3
entPhysicalContainedIn.5 = 4
entPhysicalContainedIn.6 = 4
entPhysicalContainedIn.7 = 1
entPhysicalContainedIn.8 = 7
entPhysicalContainedIn.9 = 8
entPhysicalContainedIn.10 = 8
entPhysicalContainedIn.11 = 1
entPhysicalContainedIn.12 = 1
entPhysicalContainedIn.13 = 1
entPhysicalContainedIn.14 = 13
entPhysicalContainedIn.15 = 14
entPhysicalContainedIn.16 = 14
entPhysicalContainedIn.17 = 15
entPhysicalContainedIn.18 = 15
entPhysicalContainedIn.19 = 15
entPhysicalContainedIn.20 = 15
entPhysicalContainedIn.21 = 15
entPhysicalContainedIn.22 = 16
entPhysicalContainedIn.23 = 16
entPhysicalContainedIn.24 = 16
entPhysicalContainedIn.25 = 16
entPhysicalContainedIn.26 = 16
entPhysicalContainedIn.27 = 1
entPhysicalContainedIn.28 = 1
entPhysicalContainedIn.29 = 28
entPhysicalContainedIn.30 = 29
entPhysicalContainedIn.31 = 30
entPhysicalContainedIn.32 = 30
entPhysicalContainedIn.33 = 30
entPhysicalContainedIn.34 = 30
entPhysicalContainedIn.35 = 30
entPhysicalContainedIn.36 = 30
entPhysicalContainedIn.37 = 30
```

Table A-2 shows the parent container for the entPhysicalDescr objects being used in this example:

Table A-2 Relationship of EntPhysicalContainedIn to entPhysicalDescr

#	entPhysicalDescr	Is Contained In...	entPhysicalContainedInValue and the Parent Container
1	uBR7246VXR chassis, Hw Serial#: 65100, Hw Revision: A		0, Topmost level, with no parent container
2	NPE 400 Card		1, Chassis
3	Chassis Slot		1, Chassis
4	I/O Dual Fast Ethernet Controller		3, Chassis Slot
5	i82543 (Livengood)		4, I/O Dual Fast Ethernet
6	i82543 (Livengood)		4, I/O Dual Fast Ethernet
7	Chassis Slot		1, Chassis
8	Dual Port Fast Ethernet (RJ45)		7, Chassis Slot
9	i82543 (Livengood)		8, Dual Port Fast Ethernet
10	i82543 (Livengood)		8, Dual Port Fast Ethernet
11	Chassis Slot		1, Chassis
12	Chassis Slot		1, Chassis
13	Chassis Slot		1, Chassis
14	MC28U_F_connector		13, Chassis Slot
15	UBR7200 CLC		14, MC28U_F connector
16	UBR7200 CLC		14, MC28U_F connector
17	BCM3138 PHY		15, UBR7200 CLC
18	BCM3138 PHY		15, UBR7200 CLC

Table A-2 Relationship of EntPhysicalContainedIn to entPhysicalDescr (continued)

#	entPhysicalDescr	Is Contained In...	entPhysicalContainedInValue and the Parent Container
19	BCM3138 PHY		15, UBR7200 CLC
20	BCM3138 PHY		15, UBR7200 CLC
21	BCM3034 PHY		15, UBR7200 CLC
22	BCM3138 PHY		16, UBR7200 CLC
23	BCM3138 PHY		16, UBR7200 CLC
24	BCM3138 PHY		16, UBR7200 CLC
25	BCM3138 PHY		16, UBR7200 CLC
26	BCM3034 PHY		16, UBR7200 CLC
27	Chassis Slot		1, Chassis
28	Chassis Slot		1, Chassis
29	MC16E		28, Chassis Slot
30	BCM3210 ASIC		29, MC16E
31	BCM3137 PHY		30, BCM3210 ASIC
32	BCM3137 PHY		30, BCM3210 ASIC
33	BCM3137 PHY		30, BCM3210 ASIC
34	BCM3137 PHY		30, BCM3210 ASIC
35	BCM3137 PHY		30, BCM3210 ASIC
36	BCM3137 PHY		30, BCM3210 ASIC
37	BCM3033 PHY		30, BCM3210 ASIC

Step 4 (Optional) If a parent object contains multiple children that are the same type of object, such as a router that contains multiple line card slots (Chassis Slots), use the entPhysicalParentRelPos objects to organize the child objects into their proper order. The entPhysicalParentRelPos objects contain an integer that shows the sequential order of the child objects. This integer typically starts incrementing from 0, so that it matches the actual numbering of the physical objects (slot 0 has an entPhysicalParentRelPos value of 0, slot 1 has an entPhysicalParentRelPos value of 1, and so forth).

Note If entPhysicalParentRelPos contains –1, then the object does not have an identifiable relationship with the other objects.

Table A-3 shows how the entPhysicalDescr objects that refer to chassis slots can be put into their physical order by using their entPhysicalParentRelPos values. For example, entPhysicalDescr.13 has an entPhysicalParentRelPos value of 4, which indicates that this slot is slot 4/0 in the router chassis.

Table A-3 Using entPhysicalParentRelPos to Order entPhysicalDescr Objects

#	entPhysicalDescr	entPhysicalContainedIn	entPhysicalParentRelPos	Physical Slot #
1	uBR7246VXR chassis	0 = TopLevel	-1	N/A
2	NPE 400 Card	1 = Chassis	-1	None
3	Chassis Slot	1 = Chassis	0	Slot 0/0
7	Chassis Slot	1 = Chassis	1	Slot 1/0
11	Chassis Slot	1 = Chassis	2	Slot 2/0
12	Chassis Slot	1 = Chassis	3	Slot 3/0
13	Chassis Slot	1 = Chassis	4	Slot 4/0
27	Chassis Slot	1 = Chassis	5	Slot 5/0
28	Chassis Slot	1 = Chassis	6	Slot 6/0

Step 5 (Optional) To map a physical interface to its ifIndex, which is defined in IF-MIB and used in other MIBs to uniquely identify a logical interface, use the entAliasMappingIdentifier object. If virtual interfaces are also configured on a cable interface line card, this table shows the mapping between the upstream's physical connector and its logical interface.

For example, the following shows the entAliasMappingIdentifier values for the router used in this example. In this example, entPhysicalDescr.5 (which Table A-1 identifies as the FastEthernet0/0 interface) maps to an ifIndex value of 1.

```
entAliasMappingIdentifier.5.0 = ifIndex.1
entAliasMappingIdentifier.6.0 = ifIndex.2
entAliasMappingIdentifier.9.0 = ifIndex.3
entAliasMappingIdentifier.10.0 = ifIndex.4
entAliasMappingIdentifier.15.0 = ifIndex.5
entAliasMappingIdentifier.16.0 = ifIndex.6
entAliasMappingIdentifier.17.0 = ifIndex.8
entAliasMappingIdentifier.18.0 = ifIndex.9
entAliasMappingIdentifier.19.0 = ifIndex.10
entAliasMappingIdentifier.20.0 = ifIndex.11
entAliasMappingIdentifier.21.0 = ifIndex.12
entAliasMappingIdentifier.22.0 = ifIndex.13
entAliasMappingIdentifier.23.0 = ifIndex.14
entAliasMappingIdentifier.24.0 = ifIndex.15
entAliasMappingIdentifier.25.0 = ifIndex.16
entAliasMappingIdentifier.26.0 = ifIndex.17
entAliasMappingIdentifier.30.0 = ifIndex.7
entAliasMappingIdentifier.31.0 = ifIndex.18
entAliasMappingIdentifier.32.0 = ifIndex.19
entAliasMappingIdentifier.33.0 = ifIndex.20
entAliasMappingIdentifier.34.0 = ifIndex.21
entAliasMappingIdentifier.35.0 = ifIndex.22
entAliasMappingIdentifier.36.0 = ifIndex.23
entAliasMappingIdentifier.37.0 = ifIndex.24
```

Generating SNMP Traps

This section describes how to configure the Cisco CMTS router to generate SNMP traps when certain events or conditions occur on the router. To use SNMP commands to configure the router to generate SNMP traps, you must define at least one target host to receive the traps, using the following procedure:

Tip You can also use the command-line interface (CLI) to enable and configure the generation of traps on the router. For information on using the CLI, see the "Enabling Notifications" section on page 4-2.

Step 1 Create an entry in the snmpTargetAddrTable, which is defined in SNMP-TARGET-MIB, for each host that is to receive traps. Each entry contains the following objects:

- snmpTargetAddrName—Unique string, up to 32 characters long, that identifies this host.
- snmpTargetAddrTDomain—The TCP/IP transport service to be used when delivering traps to this host, typically snmpUDPDomain.
- snmpTargetAddrTAddress—The transport address for the host, typically a six-octet value that is composed of the host's four-byte IP address followed by the two-byte UDP port number to which the traps should be sent.
- snmpTargetAddrTimeout—Maximum period of time, in hundredths of a second, that the Cisco CMTS router waits for a response from the host (if any). The default is 1500 (15 seconds).
- snmpTargetAddrRetryCount—Default number of times that the Cisco CMTS router resends a trap if a response is not received within the timeout period. The default value is 3 retries.
- snmpTargetAddrTagList—List of tags (defined below) that should be associated with this particular target host. If a host's tag value matches an snmpNotifyTag value, the host receives the types of notifications that are defined by the corresponding snmpNotifyType.
- snmpTargetAddrParams—Arbitrary string, up to 32 characters long, that identifies an entry in the snmpTargetParamsTable, which defines the parameters to be used in generating traps.
- snmpTargetAddrStorageType—Type of storage to be used for this row entry: volatile(2), nonVolatile(3), permanent(4), or readOnly(5). The default is nonVolatile(4).
- snmpTargetAddrRowStatus—Must be set to createAndGo(4) or createAndWait(5) to create this row entry. This object must be set only after all of the other entries in the row have been set.

Step 2 Create an entry in the snmpTargetParamsTable, which is defined in SNMP-TARGET-MIB, to define the SNMP parameters that the router should use when generating SNMP notifications. Each entry contains the following objects:

- snmpTargetParamsName—Unique string, up to 32 characters long, that defines this particular entry. This string is also used in the snmpTargetAddrParams to define the parameters to be used when sending traps to any particular host.
- snmpTargetParamsMPModel—Version of SNMP to be used in sending this trap: 0=SNMPv1, 1=SNMPv2c, and 3=SNMPv3.
- snmpTargetParamsSecurityModel—Version of SNMP security to be used in sending traps: 0=SNMPv1, 1=SNMPv2c, and 3=SNMPv3.
- snmpTargetParamsSecurityName—String, up to 32 characters long, to be used in identifying the Cisco CMTS router when sending traps.
- snmpTargetParamsSecurityLevel—Type of security to be used when sending traps: noAuthNoPriv(1), authNoPriv(2), and authPriv(3).

- snmpTargetParamsStorageType—Type of storage to be used for this row entry: volatile(2), nonVolatile(3), permanent(4), or readOnly(5). The default is nonVolatile(4).
- snmpTargetParamsRowStatus—Must be set to createAndGo(4) or createAndWait(5) to create this row entry. This object must be set only after all of the other entries in the row have been set.

Step 3 Create an entry in the snmpNotifyTable, which is defined in the SNMP-NOTIFICATION-MIB. Each row in this table contains the following objects, which define a set of host targets that are to receive traps:

- snmpNotifyName—Unique string, up to 32 characters, that identifies this particular row entry.
- snmpNotifyTag—Arbitrary string, up to 255 characters, that identifies the set of hosts to receive traps. This tag value is matched against the snmpTargetAddrTagList object to determine which hosts should receive which traps.
- snmpNotifyType—Defines the type of trap to be set: trap(1) or inform(2). The default is trap(1).
- snmpNotifyStorageType—Type of storage to be used for this row entry: volatile(2), nonVolatile(3), permanent(4), or readOnly(5). The default is nonVolatile(4).
- snmpNotifyRowStatus—Must be set to createAndGo(4) or createAndWait(5) to create this row entry. This object must be set only after all of the other entries in the row have been set.

Step 4 Optionally create rows in the snmpNotifyFilterProfileTable and snmpNotifyFilterTable, which are defined in the SNMP-NOTIFICATION-MIB. These tables create notification filters that limit the types of notifications that the router sends to particular hosts.

Step 5 Optionally enable traps and notifications to be sent. Most other MIBs include their own objects of NOTIFICATION-TYPE that enable or disable feature-specific traps. These notification objects also define the varbinds that are sent with each trap, which contain the specific information about the event that occurred.

For example, the CISCO-CABLE-SPECTRUM-MIB includes an ccsHoppingNotification object that enables or disables traps that are sent when a frequency hop occurs, or when the channel width or modulation profile changes. These traps provide the conditions of the upstream at the time of the hop, the old and new center frequencies, the old and new channel widths, and the old and new modulation profiles, as appropriate.

A number of notifications and traps can also be enabled using CLI commands. Table A-4 lists some of the most common traps, how they can be enabled through the CLI, and the situations that generate these traps.

Table A-4 Common Notifications and Traps

Type of Trap	Configuration Command to Enable	Description
Configuration Changes	`snmp-server enable traps entity`	When ENTITY traps are enabled, the router generates an entConfigChange trap when the information in any of the following tables in the ENTITY-MIB changes: • entPhysicalTable • entAliasMappingTable • entPhysicalContainsTable **Note** The SNMP manager should also regularly poll the entLastChangeTime object to detect whether traps were missed due to throttling or transmission loss.
Environmental Changes	`snmp-server enable traps envmon`	When ENVMON traps are enabled, the router generates the following traps (defined in CISCO-ENVMON-MIB) to notify you of potential environmental problems: • 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.
FRU Status Changes	`snmp-server enable traps fru-ctrl`	When FRU traps are enabled, the router generates the following traps (defined in CISCO-ENTITY-FRU-CONTROL-MIB) to notify the host of any changes in field-replaceable units (FRUs): • cefcModuleStatusChange—The operational status (cefcModuleOperStatus) of a FRU changed. • cefcFRUInserted—A FRU was inserted in the chassis. • cefcFRURemoved—A FRU was removed from the chassis.
Alarm is Asserted or Cleared	`snmp-server enable traps alarms`	When ALARM traps are enabled, the router generates a trap whenever an alarm is asserted or cleared for physical entities that are defined in the entPhysicalTable in the ENTITY-MIB.
SYSLOG Message is Generated	`snmp-server enable traps syslog`	By default, the Cisco CMTS router logs a SYSLOG message each time an alarm is asserted or cleared. To also generate a separate trap when any SYSLOG message is logged, set the clogNotificationsEnabled object to true(1). Set the clogMaxSeverity object in CISCO-SYSLOG-MIB to the maximum severity level for the SYSLOG messages that are to be stored in the CISCO-SYSLOG-MIB and for which notifications should generated. The default is 5 (warning), which indicates that SYSLOG messages of severity levels 1 through 5 are processed by the MIB.

Monitoring SYSLOG Messages

The CISCO-SYSLOG-MIB defines a number of objects that store the SYSLOG messages that the Cisco CMTS router generates during its normal operations. You can regularly poll this MIB to obtain the list of SYSLOG messages that have been generated.

Message Table Objects

When enabled, SYSLOG messages are stored as an entry in the clogHistoryTable. Each clogHistoryEntry contains the following objects for each message that is stored:

- clogHistIndex—Index number that uniquely identifies each SYSLOG message that is stored in the table. This index is a 32-bit value that continually increases until it reaches its maximum value, at which point it wraps around back to 1.
- clogHistFacility—Facility identifier, up to 20 characters, of the SYSLOG message.
- clogHistSeverity—Severity level of the SYSLOG message, as defined by the SyslogSeverity textual convention, which ranges from 1 (emergency) to 8 (debug).

Note The severity numbers used in the SyslogSeverity and clogHistSeverity objects are one more than the numbers used in the actual SYSLOG messages. For example, an error SYSLOG message has a severity of 3, but SyslogSeverity uses 4 for error messages.

- clogHistMsgName—Mnemonic that identifies this SYSLOG message, up to 30 characters. If the mnemonic is longer than 30 characters, it is truncated to 29 characters and an asterisk (*) is appended to the end of the message to indicate that it has been truncated.
- clogHistMsgText—Actual text of the SYSLOG message, up to 255 characters, as it would appear in the console and SYSLOG logs. If a message is longer than 255 characters, it is truncated to 254 characters and an asterisk (*) is appended to the end of the message to indicate it has been truncated.
- clogHistTimestamp—Time stamp, in terms of sysUpTime, for when the SYSLOG message was generated.

Control Objects

The following objects in the CISCO-SYSLOG-MIB control the number and type of messages that are stored in the clogHistoryTable:

- clogMaxSeverity—Maximum severity level for the SYSLOG messages that are processed by this MIB. The default is 5 (warning), which indicates that SYSLOG messages of severity levels 1 through 5 are processed by the MIB.
- clogMsgIgnores—Number of SYSLOG messages that were ignored because it had a severity level greater than that specified by the clogMaxSeverity.
- clogMsgDrops—Number of SYSLOG messages that were dropped and not stored in the clogHistoryTable because of a lack of resources.
- clogHistTableMaxLength—Maximum number of SYSLOG messages that can be stored in the clogHistoryTable. When the table is full, the oldest message in the table is deleted to make room when a new SYSLOG message is generated. The valid range is 0 to 500, with a default of 1.

- clogHistMsgsFlushed—Number of entries that have been removed from the clogHistoryTable to make room for new entries. If this object is continually increasing, it indicates that you either need to increase the size of the table (clogHistTableMaxLength) or need to poll the table more frequently.

SYSLOG Notifications

You can configure the Cisco CMTS router so that it generates an SNMP notification when a SYSLOG message is generated. The notification sends an clogMessageGenerated object, which contains the following objects that identify the SYSLOG message:

- clogHistFacility
- clogHistSeverity
- clogHistMsgName
- clogHistMsgText
- clogHistTimestamp

To enable SYSLOG notifications using CLI commands, give the following command in global configuration mode:

```
snmp-server enable traps syslog
```

To enable these notifications using SNMP commands, set the clogNotificationsEnabled object to true(1). The clogNotificationsSent object then contains the number of clogMessageGenerated notifications that have been sent.

Example

The following example shows typical output from the CISCO-SYSLOG-MIB when using the SNMP utilities that are standard on many UNIX-based systems. This router uses the default configuration, where only one SYSLOG message is stored in the clogHistoryTable. The table currently contains an entry with the index of 25, and clogHistMsgsFlushed shows that the 24 previous messages have already been flushed from the table.

```
csh% getmany -v2c 10.10.11.12 public ciscoSyslogMIB

    clogNotificationsSent.0 = 0
    clogNotificationsEnabled.0 = false(2)
    clogMaxSeverity.0 = warning(5)
    clogMsgIgnores.0 = 199
    clogMsgDrops.0 = 0
    clogHistTableMaxLength.0 = 1
    clogHistMsgsFlushed.0 = 24
    clogHistFacility.25 = UBR7200
    clogHistSeverity.25 = error(4)
    clogHistMsgName.25 = AUTH_REJECT_PERMANENT_AUTHORI*
    clogHistMsgText.25 = <132>CMTS[DOCSIS]:<66030108>  Auth Reject - Permanent
    Authorization Failure . CM Mac Addr <000C.AB01.CD89>
    clogHistTimestamp.25 = 4452551

csh%
```

Displaying Information About Cable Modems

This section describes how to obtain information about one or all cable modems:

- "Displaying Current Status for Cable Modems" section on page A-17
- "Displaying Information About Burst and Station Maintenance Intervals" section on page A-18
- "Logging and Displaying Deleted Service Flows" section on page A-19

Displaying Current Status for Cable Modems

To display the current status for one or more cable modems, display the docsIfCmtsCmStatusValue object from the docsIfCmtsCmStatusTable, which is in the DOCS-IF-MIB. This object contains the following states for each cable modem:

- other(1)—Any state other than those listed below, such as offline.
- ranging(2)—The cable modem has sent an initial ranging request to the Cisco CMTS, but has not yet completed the ranging process.
- rangingAborted(3)—The Cisco CMTS has sent a Ranging Abortion message to the cable modem, requiring it to restart the ranging process.
- rangingComplete(4)—The Cisco CMTS has sent a Ranging Complete message to the cable modem, allowing it to continue on to the registration process.
- ipComplete(5)—The cable modem has sent a DHCP broadcast, and the Cisco CMTS has forwarded the DHCP reply, with an assigned IP address, to the cable modem.
- registrationComplete(6)—The Cisco CMTS has sent a Registration Response message to the cable modem, indicating that the cable modem has completed the registration process and can now come online and forward traffic from its CPE devices.
- accessDenied(7) —The Cisco CMTS has sent a Registration Aborted message to the cable modem, indicating that the provisioning system is not allowing the cable modem and its CPE devices to come online.

To display the current status of one or more cable modems, use the following procedure:

Step 1 Poll the docsIfCmtsCmStatusMacAddress object from the docsIfCmtsCmStatusTable to obtain the MAC addresses for the known cable modems:

```
csh% getmany -v2c 10.10.17.91 public docsIfCmtsCmStatusMacAddress

docsIfCmtsCmStatusMacAddress.671745 = 00 0a ff 01 44 5e
docsIfCmtsCmStatusMacAddress.671746 = 00 0b fe 01 18 5e
docsIfCmtsCmStatusMacAddress.671747 = 00 0c fd 21 bb 54
docsIfCmtsCmStatusMacAddress.671748 = 00 0d fc 89 5f a9
docsIfCmtsCmStatusMacAddress.671749 = 00 0e fb 89 6b fd
docsIfCmtsCmStatusMacAddress.671750 = 00 0f fa 89 5c 6d
docsIfCmtsCmStatusMacAddress.671751 = 00 00 f0 89 5d 35

csh%
```

Step 2 Poll the docsIfCmtsCmStatusValue objects to obtain the current status of those cable modems:

```
csh% getmany -v2c 10.10.17.91 public docsIfCmtsCmStatusValue

docsIfCmtsCmStatusValue.671745 = registrationComplete(6)
```

```
docsIfCmtsCmStatusValue.671746 = registrationComplete(6)
docsIfCmtsCmStatusValue.671747 = registrationComplete(6)
docsIfCmtsCmStatusValue.671748 = registrationComplete(6)
docsIfCmtsCmStatusValue.671749 = accessDenied(7)
docsIfCmtsCmStatusValue.671750 = registrationComplete(6)
docsIfCmtsCmStatusValue.671751 = registrationComplete(6)

csh%
```

Step 3 Use the index value of the docsIfCmtsCmStatusValue and docsIfCmtsCmStatusMacAddress objects to find the current status of any particular cable modem. For example, the output displayed by this example shows that the cable modem with the MAC address of 00.0E.FB.89.6B.FD, which has the index of 671749, is currently marked with a status of accessDenied(7).

```
docsIfCmtsCmStatusMacAddress.671749 = 00 0e fb 89 6b fd
...
docsIfCmtsCmStatusValue.671749 = accessDenied(7)
```

Displaying Information About Burst and Station Maintenance Intervals

To display information about the burst and station maintenance intervals being used on an upstream, poll the cdxUpInfoElemStatsIEType object from the CISCO-DOCS-EXT-MIB. This object is a sequence of six entries that are indexed by the upstream's ifDescr value:

- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.1—Displays the current number of mini-slots being used for request bursts (reqIE), which are used for bandwidth requests.
- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.2—Displays the current number of mini-slots being used for request/data bursts (reqOrDataIE), which are used for bandwidth or short data packet requests.
- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.3—Displays the current number of mini-slots being used for initial maintenance bursts (initMtnIE), which are reserved for new cable modems that want to come online.
- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.4—Displays the current number of mini-slots being used for station maintenance bursts (stnMtnIE), which are used for keepalive and network maintenance messages.
- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.5—Displays the current number of mini-slots being used for short data grant bursts (shortGrantIE), which are used for short data grants.
- cdxUpInfoElemStatsIEType.*upstream-ifDescr*.6—Displays the current number of mini-slots being used for long data grant bursts (longGrantIE), which are used for large data requests.

To obtain this information, use the following procedure:

Step 1 Obtain the ifIndex for the desired upstream. This can be done by requesting a GET request for ifDescr. For example, the following shows sample output from a Cisco uBR7246VXR router that has one Fast Ethernet port adapter and one Cisco uBR-MC16C cable interface card installed:

```
csh% getmany -v2c 10.10.10.13 public ifDescr

ifDescr.1 = FastEthernet0/0
ifDescr.2 = FastEthernet0/1
ifDescr.3 = FastEthernet1/0
ifDescr.4 = FastEthernet1/1
ifDescr.5 = Cable4/0
```

```
ifDescr.8 = Cable4/0-upstream0
ifDescr.9 = Cable4/0-upstream1
ifDescr.10 = Cable4/0-upstream2
ifDescr.11 = Cable4/0-upstream3
ifDescr.12 = Cable4/0-upstream4
ifDescr.13 = Cable4/0-upstream5

csh%
```

Step 2 Use the ifIndex for the desired upstream as the index for each of the six cdxUpInfoElemStatsIEType objects. The following example uses ifDescr for upstream 0 on the Cisco uBR-MC16C card:

```
csh% getmany -v2c 10.10.10.13 public cdxUpInfoElemStatsIEType.8

cdxUpInfoElemStatsIEType.8.reqIE = 76826109
cdxUpInfoElemStatsIEType.8.reqOrDataIE = 0
cdxUpInfoElemStatsIEType.8.initMtnIE = 494562
cdxUpInfoElemStatsIEType.8.stnMtnIE = 47447
cdxUpInfoElemStatsIEType.8.shortGrantIE = 242
cdxUpInfoElemStatsIEType.8.longGrantIE = 29116

csh%
```

Note The Cisco CMTS supports, but does not use, request/data bursts, so the output for the reqOrDataIE type is always 0.

Logging and Displaying Deleted Service Flows

The DOCSIS 2.0 specifications require that the CMTS maintains a log table of deleted DOCSIS 1.1 or DOCSIS 2.0 service flows. Entries stay in this table until they either age out, or until the table becomes full, at which time the oldest entries are deleted to make room for the newest ones.

Use the following procedure to enable logging of deleted service flows, and then to display the entries in the log table (docsQosServiceFlowLogTable in the DOCS-QOS-MIB).

Step 1 On the Cisco CMTS router console, enable logging of deleted service flows by giving the **cable sflog** command at the global configuration prompt. This command has the following syntax:

cable sflog max-entry *number* **entry-duration** *time*

You must specify the following parameters:

- **max-entry** *number*—Specifies the maximum number of entries in the service flow log. When the log becomes full, the oldest entries are deleted to make room for new entries. The valid range is 0 to 59999, with a default of 0 (which disables service flow logging).

  Note The **max-entry** value applies to the entire chassis on the Cisco uBR7100 series and Cisco uBR7200 series routers, but applies to individual cable line cards on the Cisco uBR10012 router.

- **entry-duration** *time*—Specifies how long, in seconds, entries can remain in the service flow log. The CMTS deletes entries in the log that are older than this value. The valid range is 1 to 86400 seconds, with a default value of 3600 seconds (1 hour).

For example, the following enables logging of deleted service flows with a table that has room for 20,000 entries, and that automatically deletes entries after they have been in the table for two hours:

```
Router(config)# cable sflog max-entry 20000 entry-duration 7200
```

Step 2 At regular intervals, the network management station should poll the docsQosServiceFlowLogTable to collect the information about the deleted service flows. The table entries are indexed by a unique 32-bit index, which wraps around to 0 when it reaches its maximum value.

The following example shows that the docsQosServiceFlowLogTable contains two entries for two deleted service flows:

```
csh% getmany -v2c 10.17.16.1 public docsQosServiceFlowLogTable
docsQosServiceFlowLogIfIndex.180001 = 10
docsQosServiceFlowLogIfIndex.180002 = 10
docsQosServiceFlowLogSFID.180001 = 3
docsQosServiceFlowLogSFID.180002 = 4
docsQosServiceFlowLogCmMac.180001 = 00 00 39 42 b2 56
docsQosServiceFlowLogCmMac.180002 = 00 00 39 42 b2 56
docsQosServiceFlowLogPkts.180001 = 0
docsQosServiceFlowLogPkts.180002 = 0
docsQosServiceFlowLogOctets.180001 = 0
docsQosServiceFlowLogOctets.180002 = 0
docsQosServiceFlowLogTimeDeleted.180001 = 58800
docsQosServiceFlowLogTimeDeleted.180002 = 58800
docsQosServiceFlowLogTimeCreated.180001 = 9400
docsQosServiceFlowLogTimeCreated.180002 = 9400
docsQosServiceFlowLogTimeActive.180001 = 474
docsQosServiceFlowLogTimeActive.180002 = 474
docsQosServiceFlowLogDirection.180001 = upstream(2)
docsQosServiceFlowLogDirection.180002 = downstream(1)
docsQosServiceFlowLogPrimary.180001 = true(1)
docsQosServiceFlowLogPrimary.180002 = true(1)
docsQosServiceFlowLogServiceClassName.180001 =
docsQosServiceFlowLogServiceClassName.180002 =
docsQosServiceFlowLogPolicedDropPkts.180001 = 0
docsQosServiceFlowLogPolicedDropPkts.180002 = 0
docsQosServiceFlowLogPolicedDelayPkts.180001 = 8
docsQosServiceFlowLogPolicedDelayPkts.180002 = 0
docsQosServiceFlowLogControl.180001 = active(1)
docsQosServiceFlowLogControl.180002 = active(1)

csh%
```

Monitoring Spectrum Management

When you are using Cisco IOS Release 12.2(8)BC2 and later releases, you can use SNMP to access the CISCO-CABLE-SPECTRUM-MIB to monitor the spectrum management activity on cable interface cards, such as the Cisco uBR-MC16S, that include a hardware-based spectrum analyzer. You can use the MIB to perform the following tasks:

- Enabling Spectrum Management, page A-21
- Displaying the Results of a Spectrum Request, page A-23

- Monitoring CNR Measurements for Individual Cable Modems, page A-24
- Displaying Information About Frequency Hops, page A-26

Enabling Spectrum Management

To enable spectrum management for an upstream on a Cisco uBR-MC16C, Cisco uBR-MC16U/X, Cisco uBR-MC28U/X, or Cisco uBR-MC5X20S/U cable interface card, create an entry in the ccsSpectrumRequestTable for the upstream. Table A-5 lists the objects that can be configured for each entry in the ccsSpectrumRequestTable table:

Table A-5 ccsSpectrumRequestTable Attributes

Attribute	Type	Description
ccsSpectrumRequestIndex	Integer32	Arbitrary index to uniquely identify each table entry.
ccsSpectrumRequestIfIndex	InterfaceIndex OrZero	IfIndex identifying an upstream on a cable interface line card that supports hardware spectrum management.
ccsSpectrumRequestMacAddr	MacAddress	MAC address to request a signal-to-noise ratio (SNR) or carrier-to-noise ration (CNR) value for a particular cable modem, or 0000.0000.0000 to request background noise for the entire spectrum.
ccsSpectrumRequestUpperFreq	CCSFrequency	Upper frequency (in KHz) for the frequency range to be monitored (5000 to 42000 KHz, with a default of 42000 KHz).
ccsSpectrumRequestLowFreq	CCSFrequency	Lower frequency (in KHz) for the frequency range to be monitored (5000 to 42000 KHz, with a default of 5000 KHz).
ccsSpectrumRequestResolution	Integer32	Requested resolution to determine how the frequency range should be sampled (12 to 37000 KHz, with a default of 60 KHz).
ccsSpectrumRequestStartTime	TimeStamp	Time when the spectrum measurement began.
ccsSpectrumRequestStoppedTime	TimeStamp	Time when the spectrum measurement finished.
ccsSpectrumRequestOperation	CCSRequestOp eration	Starts a new spectrum management request or aborts the current one.
ccsSpectrumRequestOperState	CCSRequestOp erState	Provides the operational state of the current spectrum management request.
ccsSpectrumRequestStatus	RowStatus	Controls the modification, creation, and deletion of table entries.

To enable spectrum management on an upstream, use the following procedure:

Step 1 Obtain the ifIndex for the desired upstream. This can be done by requesting a GET request for ifDescr. For example, the following shows sample output from a Cisco uBR7246VXR router that has one Fast Ethernet port adapter and one Cisco uBR-MC16S cable interface card installed in slot 6:

```
csh% getmany -v2c 10.10.10.13 public ifDescr

ifDescr.1 = FastEthernet0/0
ifDescr.2 = FastEthernet0/1
ifDescr.3 = FastEthernet1/0
ifDescr.4 = FastEthernet1/1
ifDescr.5 = Cable6/0
ifDescr.6 = Cable6/0-upstream0
ifDescr.7 = Cable6/0-upstream1
ifDescr.8 = Cable6/0-upstream2
ifDescr.9 = Cable6/0-upstream3
ifDescr.10 = Cable6/0-upstream4
ifDescr.11 = Cable6/0-upstream5

csh%
```

Step 2 Create a row in the ccsSpectrumRequestTable for the desired upstream. At a minimum, you must create the row in the wait condition and then configure the upstream ifIndex before activating the row.

The following example shows a row being created for upstream 2 (ifIndex 8). The arbitrary row index of 8 has been chosen for this row—ensure that the row index you choose is not currently in use.

```
csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestStatus.8 -i 5
ccsSpectrumRequestStatus.8 = wait(5)

csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestIfIndex.8 -i 8
ccsSpectrumRequestIfIndex.8 = 8

csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestStatus.8 -i 1
ccsSpectrumRequestStatus.8 = active(1)

csh%
```

Note If you attempt to use an IfIndex that does not specify an upstream on a cable interface line card that supports hardware spectrum management, the SET request fails with an invalid value error.

Step 3 Display the current configuration of the new row entry, to verify that the default parameters are acceptable:

```
csh% getmany -v2c 10.10.10.13 public ccsSpectrumRequestTable

ccsSpectrumRequestIfIndex.8 = 8
ccsSpectrumRequestMacAddr.8 = 00 00 00 00 00 00
ccsSpectrumRequestLowFreq.8 = 5000
ccsSpectrumRequestUpperFreq.8 = 42000
ccsSpectrumRequestResolution.8 = 60
ccsSpectrumRequestOperation.8 = none(0)
ccsSpectrumRequestOperState.8 = idle(0)
ccsSpectrumRequestStartTime.8 = 0
ccsSpectrumRequestStoppedTime.8 = 0
ccsSpectrumRequestStatus.8 = active(1)

csh%
```

Step 4 By default, ccsSpectrumRequestMacAddr is set to all zeros, which requests background noise for the entire upstream. To monitor the CNR for a particular cable modem, set ccsSpectrumRequestMacAddr to its MAC address:

```
csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestMacAddr.8 -o '00 01 64 ff eb 95'
ccsSpectrumRequestMacAddr.3 = 00 01 64 ff eb 95

csh% getmany -v2c 10.10.10.13 public ccsSpectrumRequestTable

ccsSpectrumRequestIfIndex.8 = 8
ccsSpectrumRequestMacAddr.8 = 00 01 64 ff eb 95
ccsSpectrumRequestLowFreq.8 = 5000
ccsSpectrumRequestUpperFreq.8 = 42000
ccsSpectrumRequestResolution.8 = 60
ccsSpectrumRequestOperation.8 = none(0)
ccsSpectrumRequestOperState.8 = idle(0)
ccsSpectrumRequestStartTime.8 = 0
ccsSpectrumRequestStoppedTime.8 = 0
ccsSpectrumRequestStatus.8 = active(1)

csh%
```

Step 5 If any other parameters need to be changed from their default values, change them to the desired values. For example, the following shows the frequency range being changed from the default range (5 MHz to 42 MHz) to 20 MHz to 28 MHz:

```
csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestLowFreq.8 -i 20000
ccsSpectrumRequestLowFreq.8 = 20000

csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestUpperFreq.8 -i 28000
ccsSpectrumRequestUpperFreq.8 = 28000

csh%
```

Step 6 When all parameters are correct, set the ccsSpectrum RequestOperation object to start(1) to begin spectrum monitoring of the upstream:

```
csh% setany -v2c 10.10.10.13 private ccsSpectrumRequestOperation.8 -i 1
ccsSpectrumRequestOperation.8 = start(1)

csh%
```

Displaying the Results of a Spectrum Request

To monitor the results of a spectrum request, display the objects in the corresponding row in the ccsSpectrumDataTable (which displays the same information as that shown by the **show controllers cable upstream spectrum** command). Table A-6 lists the objects that are stored in this table:

Table A-6 ccsSpectrumDataTable Attributes

Attribute	Type	Description
ccsSpectrumDataFreq	CCSMeasured Frequency	Frequency in KHz for which this power measurement was made
ccsSpectrumDataPower	INTEGER	Measured received power for the given frequency (-50 to 50 dBmV)

To display the results of a spectrum request, use the following procedure:

Step 1 Create and activate a spectrum request by adding a row to the ccsSpectrumRequestTable, as shown in the "Enabling Spectrum Management" section on page A-21.

Step 2 Display the entries in the ccsSpectrumDataTable:

```
csh% getmany -v2c 10.10.10.13 public ccsSpectrumDataTable

ccsSpectrumDataFreq.8.20001 = 20001
ccsSpectrumDataFreq.8.20121 = 20121
ccsSpectrumDataFreq.8.20241 = 20241
ccsSpectrumDataFreq.8.20361 = 20361

...

ccsSpectrumDataFreq.8.27561 = 27561
ccsSpectrumDataFreq.8.27681 = 27681
ccsSpectrumDataFreq.8.27801 = 27801
ccsSpectrumDataFreq.8.27921 = 27921

ccsSpectrumDataPower.8.20001 = -43
ccsSpectrumDataPower.8.20121 = -50
ccsSpectrumDataPower.8.20241 = -47
ccsSpectrumDataPower.8.20361 = -46

...

ccsSpectrumDataPower.8.27561 = -47
ccsSpectrumDataPower.8.27681 = -44
ccsSpectrumDataPower.8.27801 = -46
ccsSpectrumDataPower.8.27921 = -42

csh%
```

Note The entries in the ccsSpectrumDataTable are indexed by the row number for the spectrum request entry in the ccsSpectrumRequestTable and by the frequency (in KHz) at which the power measurement was made.

Step 3 Use the ccsSpectrumDataFreq values to determine the frequencies at which power measurements were made. Then use the frequency value, as well as the ccsSpectrumRequestTable row entry, to determine the specific power measurement for any particular frequency.

For example, the following line shows that the power measurement for the upstream specified in row 3 of the ccsSpectrumRequestTable is –46 dBmV at 27.801 MHz:

```
ccsSpectrumDataPower.8.27801 = -46
```

Monitoring CNR Measurements for Individual Cable Modems

To obtain the carrier-to-noise ratio (CNR) for an individual cable modem, create and activate an entry in the ccsSNRRequestTable. Table A-7 lists the objects that can be configured for each entry in this table:

Table A-7 ccsSNRRequestTable Attributes

Attribute	Type	Description
ccsSNRRequestIndex	Integer32	Arbitrary index to uniquely identify each table entry.
ccsSNRRequestMacAddr	MacAddress	MAC address of the remote online cable modem being reported on.
ccsSNRRequestSNR	Integer32	SNR value, in dB, that has been measured. This value is 0 when the operation state is "running."
ccsSNRRequestOperation	CCSRequestOperation	Sets the current operation: start, pending, running, or abort.
ccsSNRRequestOperState	CCSRequestOperState	Reports on the current operation state: idle, pending, running, noError, aborted, notOnLine, invalidMac, timeOut, fftBusy, fftFailed, others.
ccsSNRRequestStartTime	TimeStamp	Contains the time when the SNR measurement operation starts.
ccsSNRRequestStoppedTime	TimeStamp	Contains the time when the SNR measurement stops.
ccsSNRRequestStatus	RowStatus	Controls the modification, creation, and deletion of table entries.

To obtain CNR information for a particular cable modem, use the following procedure:

Step 1 Create a row in the ccsSNRRequestTable for the desired cable modem. At a minimum, you must create the row in the wait condition and then configure the cable modem's MAC address before activating the row. For example:

```
csh% setany -v2c 10.10.10.13 private ccsSNRRequestStatus.200 -i 5
ccsSNRRequestStatus.200 = createAndWait(5)

csh% setany -v2c 10.10.10.13 private ccsSNRRequestMacAddr.200 -o '00 03 e3 50 9b 3d'
ccsSNRRequestMacAddr.200 = 00 03 e3 50 9b 3d

csh% setany -v2c 10.10.10.13 private ccsSNRRequestStatus.200 -i 1
ccsSNRRequestStatus.200 = active(1)

csh%
```

Step 2 Display the current configuration of the new row entry, to verify that the default parameters are acceptable:

```
csh% getmany -v2c 10.10.10.13 public ccsSNRRequestTable

ccsSNRRequestMacAddr.200 = 00 03 e3 50 9b 3d
ccsSNRRequestSNR.200 = 0
ccsSNRRequestOperation.200 = none(0)
ccsSNRRequestOperState.200 = idle(0)
ccsSNRRequestStartTime.200 = 0
ccsSNRRequestStoppedTime.200 = 0
ccsSNRRequestStatus.200 = active(1)

csh%
```

Step 3 When all parameters are correct, set the ccsSpectrum ccsSNRRequestOperation object to start(1) to begin monitoring of the cable modem:

```
csh% setany -v2c 10.10.10.13 private ccsSNRRequestOperation.200 -i 1
ccsSNRRequestOperation.200 = start(1)

csh%
```

Step 4 Repeatedly poll the ccsSNRRequestTable until ccsSNRRequestOperState shows noError, at which point ccsSNRRequestSNR shows the cable modem's current CNR value:

Note The ccsSNRRequestSNR object continues to show 0 as long as ccsSNRRequestOperState shows the state as running(2).

```
csh% getmany -v2c 10.10.10.13 public ccsSNRRequestTable

ccsSNRRequestMacAddr.200 = 00 03 e3 50 9b 3d
ccsSNRRequestSNR.200 = 0
ccsSNRRequestOperation.200 = start(1)
ccsSNRRequestOperState.200 = running(2)
ccsSNRRequestStartTime.200 = 0
ccsSNRRequestStoppedTime.200 = 0
ccsSNRRequestStatus.200 = active(1)

csh% getmany -v2c 10.10.10.13 public ccsSNRRequestTable

ccsSNRRequestMacAddr.200 = 00 03 e3 50 9b 3d
ccsSNRRequestSNR.200 = 25
ccsSNRRequestOperation.200 = start(1)
ccsSNRRequestOperState.200 = noError(3)
ccsSNRRequestStartTime.200 = 298853
ccsSNRRequestStoppedTime.200 = 298974
ccsSNRRequestStatus.200 = active(1)

csh%
```

Displaying Information About Frequency Hops

To obtain information about the most recent frequency hops on an upstream, display the objects in the ccsUpSpecMgmtTable. Table A-8 lists the attributes in this table:

Table A-8 ccsUpSpecMgmtEntry Attributes

Attribute	Type	Description
ccsUpSpecMgmtHopPriority	INTEGER	Specifies the priority of frequency, modulation profile, and channel width in determining corrective action for excessive noise on the upstream (default is frequency, modulation profile, and channel width)
ccsUpSpecMgmtSnrThres1	Integer32	Specifies the upper SNR threshold for modulation profile 1 (5–35 dB, default of 25)

Table A-8 ccsUpSpecMgmtEntry Attributes (continued)

Attribute	Type	Description
ccsUpSpecMgmtSnrThres2	Integer32	Specifies the upper SNR threshold for modulation profile 2 (5–35 dB, default of 15, and must be lower than that specified for ccsUpSpecMgmtSnrThres1)
ccsUpSpecMgmtFecCorrectThres1	Integer32	Specifies the forward error correction (FEC) correctable error threshold for modulation profile 1 (1–20%)
ccsUpSpecMgmtFecCorrectThres2	Integer32	Deprecated and no longer used
ccsUpSpecMgmtFecUnCorrectThres1	Integer32	Specifies the FEC uncorrectable error threshold for modulation profile 1 (1–20%)
ccsUpSpecMgmtFecUnCorrectThres2	Integer32	Deprecated and no longer used
ccsUpSpecMgmtSnrPollPeriod	Integer32	Deprecated and no longer used
ccsUpSpecMgmtHopCondition[1]	INTEGER	Reports the condition that triggers a frequency hop (SNR value or percentage of modems going offline)
ccsUpSpecMgmtFromCenterFreq[1]	CCSFrequency	Provides the center frequency (in KHz) before the latest frequency hop
ccsUpSpecMgmtToCenterFreq[1]	CCSFrequency	Provides the current center frequency (in KHz) after the latest frequency hop
ccsUpSpecMgmtFromBandWidth[1]	CCSFrequency	Provides the channel width (in KHz) before the latest frequency hop
ccsUpSpecMgmtToBandWidth[1]	CCSFrequency	Provides the current channel width (in KHz) after the latest frequency hop
ccsUpSpecMgmtFromModProfile[1]	Integer32	Provides the modulation profile number before the latest frequency hop
ccsUpSpecMgmtToModProfile[1]	Integer32	Provides the current modulation profile number after the latest frequency hop
ccsUpSpecMgmtSNR	Integer32	Provides the current SNR value (in dB) for the upstream

1. These objects are also sent in the notification message that is sent when a frequency hop occurs on an upstream.

To collect the frequency hopping data for one or more upstreams, use the following procedure:

Step 1 Obtain the ifIndex for the desired upstreams. This can be done by requesting a GET request for ifDescr. For example, the following shows sample output from a Cisco uBR7246VXR router with the first four upstreams on the cable interface card in slot 5/0:

```
csh% getmany -v2c 10.10.10.13 public ifDescr

...

ifDescr.24 = Cable5/0-upstream0
ifDescr.25 = Cable5/0-upstream1
ifDescr.26 = Cable5/0-upstream2
ifDescr.27 = Cable5/0-upstream3
```

```
...

csh%
```

Step 2 Display the ccsUpSpecMgmtTable. Use the ifDescr values of the desired upstreams to find the values for those upstreams. The following example shows the relevant output for the four upstreams shown above.

```
csh% getmany -v2c 10.10.10.13 public ccsUpSpecMgmtTable

...
ccsUpSpecMgmtHopPriority.24 = frqModChannel(0)
ccsUpSpecMgmtHopPriority.25 = frqModChannel(0)
ccsUpSpecMgmtHopPriority.26 = frqModChannel(0)
ccsUpSpecMgmtHopPriority.27 = frqModChannel(0)
...
ccsUpSpecMgmtSnrThres1.24 = 25
ccsUpSpecMgmtSnrThres1.25 = 25
ccsUpSpecMgmtSnrThres1.26 = 25
ccsUpSpecMgmtSnrThres1.27 = 25
...
ccsUpSpecMgmtSnrThres2.24 = 15
ccsUpSpecMgmtSnrThres2.25 = 15
ccsUpSpecMgmtSnrThres2.26 = 15
ccsUpSpecMgmtSnrThres2.27 = 15
...
ccsUpSpecMgmtFecCorrectThres1.24 = 1
ccsUpSpecMgmtFecCorrectThres1.25 = 1
ccsUpSpecMgmtFecCorrectThres1.26 = 1
ccsUpSpecMgmtFecCorrectThres1.27 = 1
...
ccsUpSpecMgmtFecCorrectThres2.24 = 1
ccsUpSpecMgmtFecCorrectThres2.25 = 1
ccsUpSpecMgmtFecCorrectThres2.26 = 1
ccsUpSpecMgmtFecCorrectThres2.27 = 1
...
ccsUpSpecMgmtFecUnCorrectThres1.24 = 1
ccsUpSpecMgmtFecUnCorrectThres1.25 = 1
ccsUpSpecMgmtFecUnCorrectThres1.26 = 1
ccsUpSpecMgmtFecUnCorrectThres1.27 = 1
...
ccsUpSpecMgmtFecUnCorrectThres2.24 = 1
ccsUpSpecMgmtFecUnCorrectThres2.25 = 1
ccsUpSpecMgmtFecUnCorrectThres2.26 = 1
ccsUpSpecMgmtFecUnCorrectThres2.27 = 1
...
ccsUpSpecMgmtSnrPollPeriod.24 = 15
ccsUpSpecMgmtSnrPollPeriod.25 = 15
ccsUpSpecMgmtSnrPollPeriod.26 = 15
ccsUpSpecMgmtSnrPollPeriod.27 = 15
...
ccsUpSpecMgmtHopCondition.24 = snr(0)
ccsUpSpecMgmtHopCondition.25 = snr(0)
ccsUpSpecMgmtHopCondition.26 = snr(0)
ccsUpSpecMgmtHopCondition.27 = snr(0)
...
ccsUpSpecMgmtFromCenterFreq.24 = 10000
ccsUpSpecMgmtFromCenterFreq.25 = 15008
ccsUpSpecMgmtFromCenterFreq.26 = 20000
ccsUpSpecMgmtFromCenterFreq.27 = 25008
...
ccsUpSpecMgmtToCenterFreq.24 = 10000
ccsUpSpecMgmtToCenterFreq.25 = 15008
ccsUpSpecMgmtToCenterFreq.26 = 20000
```

```
ccsUpSpecMgmtToCenterFreq.27 = 25008
...
ccsUpSpecMgmtFromBandWidth.24 = 1600
ccsUpSpecMgmtFromBandWidth.25 = 3200
ccsUpSpecMgmtFromBandWidth.26 = 3200
ccsUpSpecMgmtFromBandWidth.27 = 3200
...
ccsUpSpecMgmtToBandWidth.24 = 1600
ccsUpSpecMgmtToBandWidth.25 = 3200
ccsUpSpecMgmtToBandWidth.26 = 3200
ccsUpSpecMgmtToBandWidth.27 = 3200
...
ccsUpSpecMgmtFromModProfile.24 = 1
ccsUpSpecMgmtFromModProfile.25 = 1
ccsUpSpecMgmtFromModProfile.26 = 1
ccsUpSpecMgmtFromModProfile.27 = 1
...
ccsUpSpecMgmtToModProfile.24 = 2
ccsUpSpecMgmtToModProfile.25 = 2
ccsUpSpecMgmtToModProfile.26 = 2
ccsUpSpecMgmtToModProfile.27 = 2
...
ccsUpSpecMgmtSNR.24 = 0
ccsUpSpecMgmtSNR.25 = 0
ccsUpSpecMgmtSNR.26 = 0
ccsUpSpecMgmtSNR.27 = 0

csh%
```

Using Flap Lists

To configure, clear, and access the flap lists on a Cisco CMTS router, use the following procedures:

- Configuring Flap List Operation Using SNMP, page A-29
- Displaying the Flap List Using SNMP, page A-30
- Displaying Flap-List Information for Specific Cable Modems, page A-32
- Clearing the Flap List and Counters Using SNMP, page A-33

Configuring Flap List Operation Using SNMP

To configure the Flap List Troubleshooting feature on the Cisco CMTS using SNMP, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. Table A-9 lists each of the configurable attributes:

Table A-9 Flap-List Configuration Attributes

Attribute	Type	Range	Description
ccsFlapListMaxSize	Integer32	1 to 65536[1]	The maximum number of modems that a flap list can support. The default is 100.
ccsFlapListCurrentSize	Integer32	1 to 65536[1]	The current number of modems in the flap list.

Table A-9 Flap-List Configuration Attributes (continued)

Attribute	Type	Range	Description
ccsFlapAging	Integer32	1 to 86400	The flap entry aging threshold in minutes. The default is 10080 minutes (180 hours or 7 days).
ccsFlapInsertionTime	Integer32	60 to 86400	The worst-case insertion time, in seconds. If a cable modem has not completed the registration stage within this interval, the cable modem is inserted into the flap list. The default value is 90 seconds.
ccsFlapPowerAdjustThreshold	Integer32	1 to 10	When the power of the modem is adjusted beyond the power adjust threshold, the modem is inserted into the flap list.
ccsFlapMissThreshold	Unsigned32	1 to 12	When a cable modem does not acknowledge this number of consecutive MAC-layer station maintenance (keepalive) messages, the cable modem is placed in the flap list.

1. The allowable range when using SNMP for these parameters is 1 to 65536 (a 32-bit value), but the valid operational range is 1 to 8191.

Displaying the Flap List Using SNMP

To display the contents of the flap list using SNMP, query the cssFlapTable in the CISCO-CABLE-SPECTRUM-MIB. This table contains an entry for each cable modem. Table A-10 briefly describes each attribute in this table.

Table A-10 cssFlapTable Attributes

Attribute	Type	Description
cssFlapMacAddr	MacAddress	MAC address of the cable modem's cable interface. Identifies a flap-list entry for a flapping cable modem.
ccsFlapUpstreamIfIndex	InterfaceIndex	Upstream being used by the flapping cable modem.
ccsFlapDownstreamIfIndex	InterfaceIndex	Downstream being used by the flapping cable modem.
ccsFlapLastFlapTime	DateAndTime	Time stamp for the last time the cable modem flapped.
ccsFlapCreateTime	DateAndTime	Time stamp that this entry was added to the table.
ccsFlapRowStatus	RowStatus	Control attribute for the status of this entry.
ccsFlapInsertionFailNum	Unsigned32	Number of times the cable modem comes up and inserts itself into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the **cable flap-list insertion-time** command or ccsFlapInsertionTime attribute. When the cable modem cannot finish registration within the insertion time (ccsFlapInsertionTime), it resends the initial maintenance packet. When the CMTS receives the packet sooner than expected, the CMTS increments this counter.
ccsFlapHitNum	Unsigned32	Number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds.)

Table A-10 cssFlapTable Attributes (continued)

Attribute	Type	Description
ccsFlapMissNum	Unsigned32	Number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. If the CMTS misses a ranging request within 25 msec, then the miss number is incremented.
ccsFlapCrcErrorNum	Unsigned32	Number of times the CMTS upstream receiver flagged a packet with a CRC error. A high value indicates that the cable upstream may have a high noise level. The modem may not be flapping yet, but this could become a problem.
ccsFlapPowerAdjustmentNum	Unsigned32	Number of times the cable modem upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power-adjustment threshold, the number is incremented.
ccsFlapTotalNum	Unsigned32	Number of times a modem has flapped, which is the sum of the following: • When ccsFlapInsertionFailNum is increased • When the CMTS receives a miss followed by a hit • When ccsFlapPowerAdjustmentNum is increased
ccsFlapResetNow	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapLastResetTime	DateAndTime	Time stamp for when all the counters for this particular entry were reset to zero.

For example, the following shows the output for ccsFlapTable when it contains entries for two cable modems with the MAC addresses of 00.07.0E.02.CA.91 (0.7.14.2.202.145) and 00.07.0E.03.68.89 (0.7.14.3.104.137):

```
csh% getmany -v2c 10.10.11.12 public ccsFlapTable

ccsFlapUpstreamIfIndex.0.7.14.2.202.145 = 17
ccsFlapUpstreamIfIndex.0.7.14.3.104.137 = 17
ccsFlapDownstreamIfIndex.0.7.14.2.202.145 = 21
ccsFlapDownstreamIfIndex.0.7.14.3.104.137 = 21
ccsFlapInsertionFails.0.7.14.2.202.145 = 2
ccsFlapInsertionFails.0.7.14.3.104.137 = 0
ccsFlapHits.0.7.14.2.202.145 = 54098
ccsFlapHits.0.7.14.3.104.137 = 54196
ccsFlapMisses.0.7.14.2.202.145 = 65
ccsFlapMisses.0.7.14.3.104.137 = 51
ccsFlapCrcErrors.0.7.14.2.202.145 = 0
ccsFlapCrcErrors.0.7.14.3.104.137 = 0
ccsFlapPowerAdjustments.0.7.14.2.202.145 = 0
ccsFlapPowerAdjustments.0.7.14.3.104.137 = 0
ccsFlapTotal.0.7.14.2.202.145 = 5
ccsFlapTotal.0.7.14.3.104.137 = 4
ccsFlapLastFlapTime.0.7.14.2.202.145 = 14 03  04 1e   07 35  10 00
ccsFlapLastFlapTime.0.7.14.3.104.137 = 14 03  04 1e   07 34  12 00
ccsFlapCreateTime.0.7.14.2.202.145 = 14 03  04 1e   07 00  2b 00
ccsFlapCreateTime.0.7.14.3.104.137 = 14 03  04 1e   07 00  2c 00
ccsFlapRowStatus.0.7.14.2.202.145 = 1
ccsFlapRowStatus.0.7.14.3.104.137 = 1
ccsFlapInsertionFailNum.0.7.14.2.202.145 = 2
ccsFlapInsertionFailNum.0.7.14.3.104.137 = 0
ccsFlapHitNum.0.7.14.2.202.145 = 54098
```

```
ccsFlapHitNum.0.7.14.3.104.137 = 54196
ccsFlapMissNum.0.7.14.2.202.145 = 65
ccsFlapMissNum.0.7.14.3.104.137 = 51
ccsFlapCrcErrorNum.0.7.14.2.202.145 = 0
ccsFlapCrcErrorNum.0.7.14.3.104.137 = 0
ccsFlapPowerAdjustmentNum.0.7.14.2.202.145 = 0
ccsFlapPowerAdjustmentNum.0.7.14.3.104.137 = 0
ccsFlapTotalNum.0.7.14.2.202.145 = 5
ccsFlapTotalNum.0.7.14.3.104.137 = 4
ccsFlapResetNow.0.7.14.2.202.145 = 2
ccsFlapResetNow.0.7.14.3.104.137 = 2
ccsFlapLastResetTime.0.7.14.2.202.145 = 14 03  04 1e   06 39  0c 00
ccsFlapLastResetTime.0.7.14.3.104.137 = 14 03  04 1e   06 39  1e 00

csh%
```

Tip To collect both the flap list configuration parameters and the contents of the flap list, perform a GET request of ccsFlapObjects.

Displaying Flap-List Information for Specific Cable Modems

To use SNMP requests to display flap-list information for a specific cable modem, use the cable modem's MAC address as the index to retrieve entries from the ccsFlapTable. Use the following procedure to retrieve flap-list entries for a particular cable modem.

DETAILED STEPS

Step 1 Convert the cable modem's MAC address into a dotted decimal string. For example, the MAC address 000C.64ff.eb95 would become 0.12.100.255.235.149.

Step 2 Use the dotted decimal version of the MAC address as the instance for requesting information from the ccsFlapTable. For example, to retrieve the ccsFlapHits, ccsFlapMisses, and ccsFlapPowerAdjustments values for this cable modem, you would make an SNMP request for the following objects:

- ccsFlapHits.0.12.100.255.235.149
- ccsFlapMisses.0.12.100.255.235.149
- ccsFlapPowerAdjustments.0.12.100.255.235.149

Example

Assume that you want to retrieve the same flap-list information as the **show cable flap-list** command for a cable modem with the MAC address of 000C.64ff.eb95:

```
Router# show cable flap-list

MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
000C.64ff.eb95  Cable3/0/U4  3314  55605 50460 0    *42175 47533 Jan 27 02:49:10

Router#
```

Use an SNMP tool to retrieve the ccsFlapTable and filter it by the decimal MAC address. For example, using the standard Unix **getone** command, you would give the following command:

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149
```

```
ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4  01 1b   02 33  1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4  01 16   03 23  22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4  01 16   03 20  18 00

csh%
```

To request just one particular value, use the decimal MAC address as the instance for that object:

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149

ccsFlapMisses.0.12.100.255.235.149 = 50736

csh %
```

Clearing the Flap List and Counters Using SNMP

To remove a cable modem from the flap list or to clear one or all of the flap-list counters, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. Table A-11 lists the attributes that clear the SNMP counters.

Table A-11 Attributes to Clear the Flap List

Attribute	Type	Description
ccsFlapResetAll	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapClearAll	Boolean	Setting this object to True (1) removes all cable modems from the flap list, and destroys all entries in the ccsFlapTable. If a modem keeps flapping, the modem is added again into the flap list as a new entry.

Note The ccsFlapLastClearTime attribute contains the date and time that the entries in the ccsFlapTable table were last cleared.

Using Subscriber Traffic Management

You can use the attributes in the CISCO-CABLE-QOS-MONITOR-MIB to configure subscriber traffic management on the Cisco CMTS router, and to display the cable modems that have violated their configured bandwidth limits. Use the following procedures to perform these tasks:

- Configuring and Displaying the Enforce Rules for Quality of Service, page A-34
- Displaying Subscribers Who Have Violated Their Enforce Rules, page A-35
- Notifications for Subscribers Who Have Violated Their Enforce Rules, page A-36

Configuring and Displaying the Enforce Rules for Quality of Service

Use the attributes in the ccqmCmtsEnforceRuleTable table to configure the QoS enforce rules that should be enforced on the Cisco CMTS router. You can also query this table to display the enforce rules that are currently defined.

Table A-12 lists the attributes that are in each row of the ccqmCmtsEnforceRuleTable table. One row entry (CcqmCmtsEnforceRuleEntry) exists for each enforce rule and is indexed by the unique rule name (ccqmCmtsEnfRuleName).

Table A-12 Attributes for the QoS Enforce Rules

Attribute	Type	Description
ccqmCmtsEnfRuleName	DisplayString	Unique name of the enforce rule, up to 15 characters long.
ccqmCmtsEnfRuleRegQoS	Unsigned32	If not set to 0, this attribute is an index into the docsIfQosProfileTable table to identify the QoS profile to be used as the registered profile with this rule.
ccqmCmtsEnfRuleEnfQos	Unsigned32	If not set to 0, this attribute is an index into the docsIfQosProfileTable table to identify the QoS profile to be used as the enforced profile that should be put into effect when subscribers violate their bandwidth limits.
ccqmCmtsEnfRuleMonDuration	Unsigned32	Time period, in minutes, of the monitoring window over which the users are monitored to determine whether they are violating their bandwidth limits. The valid range is 10 to 10,080 minutes (7 days), with a default value of 360 minutes (6 hours).
ccqmCmtsEnfRuleSampleRate	Unsigned32	How often, in minutes, the Cisco CMTS checks the subscriber's bandwidth usage to determine whether they are violating their bandwidth limits. The valid range is 10 to 120 minutes (2 hours), with a default of 15 minutes.
ccqmCmtsEnfRulePenaltyPeriod	Unsigned32	How long, in minutes, the subscriber remains in the penalty period after violating their bandwidth limits. The subscriber is forced to use the enforced QoS profile until this time period expires or until the penalty period is manually cleared on the Cisco CMTS. The valid range is 1 to 10,080 minutes, with a default of 10,080 (7 days).

Table A-12 Attributes for the QoS Enforce Rules (continued)

Attribute	Type	Description
ccqmCmtsEnfRuleByteCount	Unsigned32	Maximum number of kilobytes that the subscriber can transmit or receive (depending on the enforce rule's direction) during each monitoring window time period. If the subscriber exceeds this number of bytes, they are flagged as overconsuming and possibly subject to the penalty period. The valid range is any 32-bit integer value, with no default.
ccqmCmtsEnfRuleDirection	CCQMRuleDirection	Specifies the direction (upstream, downstream, or bidirectional) over which bytes are monitored for this enforce rule.
ccqmCmtsEnfRuleAutoEnforce	TruthValue	Specifies whether the enforced QoS profile is automatically applied when the subscriber violates the bandwidth limits. The default is False (the enforced QoS profile is not automatically applied).
ccqmCmtsEnfRuleRowStatus	RowStatus	Specifies the status of this particular row. This enforce rule entry becomes active only when the RowStatus is set to active(1). To change any of the row parameters, however, the RowStatus must first be set to notInService(2), which ends the current monitoring of users with this enforce rule. Then the row must be set back to active(1) before monitoring starts again.

Displaying Subscribers Who Have Violated Their Enforce Rules

Table A-13 lists the attributes available for each entry (ccqmEnfRuleViolateEntry) in the ccqmEnfRuleViolateTable table, which lists the subscribers who have violated their enforce rule over the configured monitoring time period.

Table A-13 Attributes for ccqmEnfRuleViolateTable Table

Attribute	Type	Description
ccqmEnfRuleViolateID	Unsigned32	Unique ID assigned to this row entry. For DOCSIS 1.0 users, this is the same value as the subscriber's service flow ID (SFID).
ccqmEnfRuleViolateMacAddr	MacAddress	MAC (hardware) address of the cable interface for the subscriber who has violated the QoS bandwidth limits.
ccqmEnfRuleViolateRuleName	DisplayString	Name of the enforce rule that is associated with this subscriber. This value can be compared to the ccqmCmtsEnfRuleName attribute to find the enforce rule assigned to this subscriber.
ccqmEnfRuleViolateByteCount	Unsigned32	Total number of kilobytes that the subscriber used during the monitoring time period. (This counter is reset whenever the enforce rule is stopped and restarted.)
ccqmEnfRuleViolateLastDetectTime	DateAndTime	The time stamp for when the Cisco CMTS determined that the subscriber had violated the enforce rule.
ccqmEnfRuleViolatePenaltyExpTime	DateAndTime	The time stamp for when the penalty period expires for this subscriber. Unless the penalty period is manually cancelled by an operator at the Cisco CMTS router, the subscriber remains in the penalty period until this date and time, at which point their original QoS profile is restored. This attribute is 0 when the subscriber's enforce rule did not include an enforced QoS Profile.

Notifications for Subscribers Who Have Violated Their Enforce Rules

To configure the Cisco CMTS router so that it sends a notification whenever a user violates the bandwidth limits in the enforce rules, set the ccqmEnfRuleViolateNotifEnable object to True. The default is False (notifications are not sent). Table A-14 lists the attributes (which are defined in the ccqmEnfRuleViolateTable table) that are sent in each notification.

Table A-14 Attributes for ccqmEnfRuleViolateNotification

Attribute	Type	Description
ccqmEnfRuleViolateMacAddr	MacAddress	MAC (hardware) address of the cable interface for the subscriber that has violated the QoS bandwidth limits.
ccqmEnfRuleViolateRuleName	DisplayString	Name of the enforce rule that is associated with this subscriber. This value can be compared to the ccqmCmtsEnfRuleName attribute to find the enforce rule assigned to this subscriber.
ccqmEnfRuleViolatePenaltyExpTime	DateAndTime	The time stamp for when the penalty period expires for this subscriber. Unless the penalty period is manually cancelled by an operator at the Cisco CMTS router, the subscriber remains in the penalty period until this date and time, at which point their original QoS profile is restored. This attribute is 0 when the subscriber's enforce rule did not include an enforced QoS Profile.
ccqmEnfRuleViolateByteCount	Unsigned32	Total number of kilobytes that the subscriber used during the monitoring time period. (This counter is reset whenever the enforce rule is stopped and restarted.)

Usage-Based Billing

The CISCO-CABLE-METERING-MIB allows for configuration of the parameters that control the metering record collection like interval, amount of metering information required, location or IP address of the collection server, and metering filename. In addition it provides for some important notifications to the NMS to indicate the success or failure of the metering collection.

Usage-Based Billing feature for the Cisco Cable Modem Termination System (CMTS), which provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

The Usage-Based Billing feature provides a standards-based, open application approach to recording and retrieving traffic billing information for DOCSIS networks. When enabled, this feature provides the following billing information about the cable modems and customer premises equipment (CPE) devices that are using the cable network:

- IP and MAC addresses of the cable modem.
- Service flows being used (both upstream and downstream service flows are tracked).
- IP addresses for the CPE devices that are using the cable modem.
- Total number of octets and packets received by the cable modem (downstream) or transmitted by the cable modem (upstream) during the collection period.
- Total number of downstream packets for the cable modem that the CMTS dropped or delayed because they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA).

Billing records are maintained in a standardized text format that the service provider can easily integrate into their existing billing applications. Service providers can use this information to determine which users might be potential customers for service upgrades, as well as those customers that might be trying to exceed their SLA limits on a regular basis.

Modes of Operation

The Usage-Based Billing feature operates in two modes:

- File Mode
- Streaming Mode

File Mode

In file mode, the CMTS collects the billing record information and writes the billing records to a file on a local file system, using a file name that consists of the router's hostname followed by a timestamp of when the file was written. A remote application can then log into the CMTS and transfer the billing record file to an external server where the billing application can access it.

The remote application can use the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP) to transfer the file. After a successful transfer, the remote application then deletes the billing record file, which signals the CMTS that it can create a new file. The remote application can either periodically log into the CMTS to transfer the billing record file, or it can wait until the CMTS sends an SNMPv3 trap to notify the application that a billing record file is available.

Usage-Based Billing Feature (File Mode)

To configure the Cisco CMTS for Usage-Based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB. Table A-15 describes each of these objects, and whether they are required or optional.

Table A-15 CISCO-CABLE-METERING-MIB Objects to be Configured for File Mode

MIB Object	Type	Description
ccmtrCollectionTable		
ccmtrCollectionType	Integer	Enables or disables the Usage-Based Billing feature. The valid values are: • 1 = none. The Usage-Based Billing feature is disabled (default). • 2 = local. The Usage-Based Billing feature is enabled and configured for file mode. • 3 = stream. The Usage-Based Billing feature is enabled and configured for streaming mode. Set ccmCollectionType to 2 (local) to enable the feature for file mode.

Table A-15 CISCO-CABLE-METERING-MIB Objects to be Configured for File Mode (continued)

MIB Object	Type	Description
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true = CPE information is present (default). • false = CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true = All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false = Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex		Indicates the source interface for the billing packets. If the ccmtrCollectionType is local(2), the IP address of this interface will be used as the CMTS IP address in the billing packets. If the ccmtrCollectionType is remote(3), the source IP address of the billing packets as well as the CMTS IP address in billing packets will be changed to the IP address of this interface. Note that metering mode must be configured to specify the source-interface for metering.

Streaming Mode

In streaming mode, the CMTS collects the billing record information and then regularly transmits the billing record file to an application on an external server, using either a non-secure TCP connection or a secure sockets layer (SSL) connection. When the external server acknowledges a successful transfer, the CMTS deletes the billing record file and begins creating a new file.

If the CMTS fails to establish a successful connection with the external server, it retries the connection between 1 and 3 times, depending on the configuration. If the CMTS continues to be unable to connect with the external server, the CMTS can send an SNMPv3 trap to notify an SNMP manager that this failure occurred.

In streaming mode, you configure the CMTS to transmit the billing record file at regular intervals. Typically, the interval chosen would depend on the number of cable modems and the size of the billing record files that the CMTS produces.

To configure the Cisco CMTS for Usage-Based Billing feature in streaming mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB. Table A-16 describes each of these objects, and whether they are required or optional.

Table A-16 CISCO-CABLE-METERING-MIB Objects to be Configured for Streaming Mode

Object	Type	Description
ccmtrCollectionTable		
ccmtrCollectionType	Integer	Enables or disables the Usage-Based Billing feature. The valid values are: • 1 = none. The Usage-Based Billing feature is disabled (default). • 2 = local. The Usage-Based Billing feature is enabled and configured for file mode. • 3 = stream. The Usage-Based Billing feature is enabled and configured for streaming mode. Set ccmCollectionType to 3 (stream) to enable the feature for streaming mode.
ccmtrCollectionIpAddress	InetAddress	IP address for the external collection server. This value must be specified.
ccmtrCollectionPort	Unsigned32	TCP port number at the external collection server to which the billing records should be sent. The valid range is 0 to 65535, but you should not specify a port in the well-known range of 0 to 1024. This value must be specified.

Note You can configure the ccmCollectionIpAddress and ccmCollectionPort objects twice, to specify a primary collection server and a secondary collection server.

ccmtrCollectionIpAddrType	InetAddressType	(Optional) Type of IP address being used for the collection server. The only valid value is ipv4, which is the default value.
ccmCollectionInterval	Unsigned32	(Optional) Specifies how often, in minutes, the billing records are streamed to the external server. The valid range is 15 to 1440 minutes (24 hours), with a default of 30 minutes. (Cisco recommends a minimum interval of 30 minutes.)
ccmtrCollectionRetries	Unsigned32	(Optional) Specifies the number of retry attempts that the CMTS will make to establish a secure connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range for *n* is 0 to 5, with a default of 0.

Note The ccmCollectionInterval and ccmCollectionRetries parameters are optional when configuring Usage-Based Billing for streaming mode with SNMP commands, but these parameters are required when configuring the feature with CLI commands.

Table A-16 CISCO-CABLE-METERING-MIB Objects to be Configured for Streaming Mode (continued)

Object	Type	Description
ccmtrCollectionSecure	TruthValue	(Optional) Specifies whether the Cisco CMTS should use a secure socket layer (SSL) connection when connecting with the billing application on the external server. The valid values are: • true(1) = The Cisco CMTS uses a SSL connection. This option is available only on CMTS software images that support Baseline Privacy Interface (BPI) encryption. • false(2) = The Cisco CMTS uses an unencrypted TCP connection. This is the default value.
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true = CPE information is present (default). • false = CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true = All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false = Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).

For complete documentation about using the Usage-Based Billing feature for Cisco CMTS, go to:

http://www.cisco.com/en/US/docs/cable/cmts/feature/ubrsamis.html

Identifying Cisco Unique Device Identifiers

In order to use UDI retrieval, the Cisco product in use must be UDI-enabled. A UDI-enabled Cisco product supports five required Entity MIB objects. The five Entity MIB v2 (RFC-2737) objects are as follows:

- entPhysicalName
- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

Although the show inventory command may be available, using that command on devices that are not UDI-enabled produces no output.

Before using the UDI Retrieval feature, you should understand the following concepts:

Unique Device Identifier Overview-Each identifiable product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have subentities like slots. An Ethernet switch might be a member of a superentity like a stack. Most Cisco entities that are orderable products will leave the factory with an assigned UDI.

The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements:

- Product identifier (PID) The PID is the name by which the product can be ordered; it has been historically called the Product Name or Part Number. This is the identifier that one would use to order an exact replacement part.
- Version identifier (VID) The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.
- Serial number (SN) The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

DOCS-DSG-IF-MIB Validation Requirements

Validation describes mandatory parameters that must be set and consistency rules so that if the data is set, the data must also conform to those rules.

This section describes the agent implementation relative to the DOCS-DSG-IF-MIB. There are rules to follow:

- All indices of MIB tables in DOCS-DSG-IF-MIB must be within the range of 1-65535 in order to keep index range consistent between SNMP and CLI to ensure inter-operability.

The valid values of a RowStatus column are:

- active—row is complete and usable.
- notInService—row is complete but not active.
- notReady—the row is missing columns required for it to be set active.

- createAndGo—create the row and have it go active in a single Set request.
- createAndWait—create the row but keep it in notInService or notReady state until activated.
- destroy—remove the row.

Table A-17 lists the capabilites of each MIB table in the DOCS-DSG-IF-MIB.

Table A-17 DOCS-DSG-IF-MIB Table Capabilities

MIB Table/Object	Maximum Access	Capability
dsgIfClassifierTable	Read-Create	Values: • CreateAndGo • CreateAndWait • Can be modified • Destroyed
dsgIfTunnelTable	Read-Create	Values: • CreateAndGo • CreateAndWait • Can be modified • Destroyed
dsgIfTunnelGrpToChannelTable	Read-Create	Values: • CreateAndGo • CreateAndWait • Can be modified • Destroyed
dsgIfDownstreamTable	Read-Write	Can be modified
dsgIfClientIdTable	Read-Create	Values: • CreateAndGo • Destroyed
dsgIfVendorParamTable	Read-Create	Values: • CreateAndGo • Destroyed
dsgIfChannelListTable	Read-Create	Values: • CreateAndGo • Destroyed
dsgIfTimerTable	Read-Create	Values: • CreateAndGo • Destroyed

APPENDIX **B**

Relationship Between MIB Objects and CLI Show Commands

This chapter shows the Management Information Base (MIB) files and their object identifiers (OIDs) that correspond to the fields that are displayed by the command-line interface (CLI) **show** commands. Because different subsystems process CLI and Simple Network Management Protocol (SNMP) commands, a slight variation should be expected between the counters returned by SNMP commands and those displayed by CLI commands.

Note Unless otherwise indicated, all SNMP counter objects are 32-bit counters. Also, all SNMP counters begin incrementing from zero when the CMTS router initially boots and continue incrementing until they wrap around to zero, or until the CMTS router is rebooted. For more information on the differences between CLI-based and SNMP-based counters, see the "SNMP-Based and CLI-Based Counters" section on page A-2.

Tip For the generic interface counters that are displayed by the **show interface** command, see the corresponding counters in the ifTable in IF-MIB.

- CISCO-CABLE-QOS-MONITOR-MIB, page B-2
- CISCO-DOCS-EXT-MIB, page B-3
- CISCO-DOCS-REMOTE-QUERY, page B-10
- DOCS-IF-MIB, page B-10
- DOCS-QOS-MIB, page B-15
- DOCS-SUBSCRIBER-MIB, page B-24

CISCO-CABLE-QOS-MONITOR-MIB

The ccqmCmtsEnforceRuleTable in CISCO-CABLE-QOS-MONITOR-MIB contains objects that show the quality of service (QoS) enforce rules that are currently configured on the Cisco CMTS. Table B-1 lists the most commonly used objects in this table and the related **show** commands:

Table B-1 Quality of Service Enforce Rules (ccqmCmtsEnforceRuleTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-CABLE-QOS-MONITOR-MIB (ciscoCableQosMonitor)		
ccqmCmtsEnforceRuleName (1.3.6.1.4.1.9.9.341.1.1.1.1.1)	**show cable qos enforce-rule**: Name	Name of this enforce rule.
ccqmCmtsEnfRuleRegQoS (1.3.6.1.4.1.9.9.341.1.1.1.1.2)	**show cable qos enforce-rule**: Reg	Pointer into the docsIfQosProfileTable for the QoS profile to be used when a subscriber registers (0 to 16383).
ccqmCmtsEnfRuleEnfQos (1.3.6.1.4.1.9.9.341.1.1.1.1.3)	**show cable qos enforce-rule**: Enf	Pointer into the docsIfQosProfileTable for the QoS profile to be used when a subscriber violates the bandwidth specified by their service level agreement (SLA) (0 to 16383).
ccqmCmtsEnfRuleMonDuration (1.3.6.1.4.1.9.9.341.1.1.1.1.4)	**show cable qos enforce-rule**: Dur (min)	Duration, in minutes, for the sliding window to be used to monitor subscribers (10 to 10080).
ccqmCmtsEnfRuleSampleRate (1.3.6.1.4.1.9.9.341.1.1.1.1.5)	**show cable qos enforce-rule**: rate (min)	Sample rate, in minutes, at which the CMTS should check a subscriber's bandwidth usage to determine whether the subscriber is overconsuming their allotted resources (10 to 120).
ccqmCmtsEnfRuleDirection (1.3.6.1.4.1.9.9.341.1.1.1.1.8)	**show cable qos enforce-rule**: Dir	Direction in which this enforce rule should be applied: upstream, downstream, or both.
ccqmCmtsEnfRuleAutoEnforce (1.3.6.1.4.1.9.9.341.1.1.1.1.9)	**show cable qos enforce-rule**: Auto enf	Indicates whether the enforced QoS profile should be automatically applied to subscribers who violate the maximum bandwidth limits during a sliding window monitoring period.

The ccqmEnfRuleViolateTable in CISCO-CABLE-QOS-MONITOR-MIB provides a snapshot of all subscribers who have violated their enforce rules. Table B-2 lists the most commonly used objects in this table and the related **show** commands:

Table B-2 Enforce Rules Violators (ccqmEnfRuleViolateID)

Object and OID	Equivalent Show Command and Field	Description
CISCO-CABLE-QOS-MONITOR-MIB (ciscoCableQosMonitor)		
ccqmEnfRuleViolateID (1.3.6.1.4.1.9.9.341.1.2.2.1.1)	**show cable subscriber-usage**: Sfid	Index for this service flow.

Table B-2 Enforce Rules Violators (ccqmEnfRuleViolateID)

Object and OID	Equivalent Show Command and Field	Description
ccqmEnfRuleViolateMacAddr (1.3.6.1.4.1.9.9.341.1.2.2.1.2)	**show cable subscriber-usage**: Mac Address	MAC address of the subscriber.
ccqmEnfRuleViolateRuleName (1.3.6.1.4.1.9.9.341.1.2.2.1.3)	**show cable subscriber-usage**: Enforce-rule Name	Name of the enforce rule being used for this subscriber.
ccqmEnfRuleViolateLastDetectTime (1.3.6.1.4.1.9.9.341.1.2.2.1.5)	**show cable subscriber-usage**: Last-detect Time	Time stamp for when the subscriber was found to have violated the enforce rule. If the enforce rule automatically applies the enforced QoS profile, this time stamp also shows the time at which the enforced QoS profile was in effect.
ccqmEnfRuleViolatePenaltyExpTime (1.3.6.1.4.1.9.9.341.1.2.2.1.6)	**show cable subscriber-usage**: Last-penalty Time	Time stamp for when the original (registered) QoS profile is scheduled to be restored to this subscriber.

CISCO-DOCS-EXT-MIB

The cdxQosCtrlUpTable in CISCO-DOCS-EXT-MIB contains a number of QoS objects that the scheduler uses to control cable modem registration on each upstream interface. Table B-3 lists the most commonly used objects in this table and the related **show** commands:

Table B-3 Quality of Service Upstream Control Objects (cdxQosCtrlUpTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxQosCtrlUpAdmissionCtrl (1.3.6.1.4.1.9.9.116.1.1.1.1.1)	N/A	Indicates whether admission control is enabled to control minimum guaranteed upstream bandwidth scheduling service requests on this upstream.
cdxQosCtrlUpMaxRsvdBWPercent (1.3.6.1.4.1.9.9.116.1.1.1.1.2)	N/A	Maximum percentage of total upstream bandwidth that is allowed to be reserved for minimum guaranteed upstream scheduling service requests on this upstream (10 to 1000 percent), when admission control is enabled.
cdxQosCtrlUpAdmissionRejects (1.3.6.1.4.1.9.9.116.1.1.1.1.3)	N/A	Total number of cable modem Registration Requests (REG-REQ) that the CMTS rejected on this upstream when admission control is enabled, because insufficient bandwidth was reserved.

Table B-3 Quality of Service Upstream Control Objects (cdxQosCtrlUpTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxQosCtrlUpReservedBW (1.3.6.1.4.1.9.9.116.1.1.1.1.4)	**show interface cable upstream**: Total channel bandwidth reserved	Total reserved bandwidth, in bits per second (bps), that is currently reserved on this upstream (0 to 102400000).
cdxQosCtrlUpMaxVirtualBW (1.3.6.1.4.1.9.9.116.1.1.1.1.5)	N/A	Maximum virtual bandwidth of this capacity, in bits per second (bps), when admission control is enabled (0 to 102400000).

The cdxCmtsServiceExtTable in CISCO-DOCS-EXT-MIB extends the information about a service ID (SID) in docsIfCmtsServiceTable. Table B-4 lists the most commonly used objects in this table and the related **show** commands:

Table B-4 Service ID Information (cdxCmtsServiceExtTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxIfCmtsServiceOutOctets (1.3.6.1.4.1.9.9.116.1.1.3.1.1)	**show interface cable sid counter verbose**: Bytes received	Total number of data packet bytes that have been sent for this SID.
cdxIfCmtsServiceOutPackets (1.3.6.1.4.1.9.9.116.1.1.3.1.2)	**show interface cable sid counter**: Packets received	Total number of data packets that have been sent for this SID.

The cdxBWQueueTable in CISCO-DOCS-EXT-MIB displays the attributes for the QoS queues in a cable interface scheduler. Table B-5 lists the most commonly used objects in this table and the related **show** commands:

Table B-5 Quality of Service Queues (cdxBWQueueTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxBWQueueNameCode (1.3.6.1.4.1.9.9.116.1.2.1.1.1)	**show interface cable upstream** and **show interface cable mac-scheduler**: Queue...	Name code (type) for this queue: cirQ(1), tbeQ(2), p0BEGrantQ(3), p1BEGrantQ(4), p2BEGrantQ(5), p3BEGrantQ(6), p4BEGrantQ(7), p5BEGrantQ(8), p6BEGrantQ(9), p7BEGrantQ(10), and rngPollQ(11).
cdxBWQueueOrder (1.3.6.1.4.1.9.9.116.1.2.1.1.2)	N/A	Relative priority of this queue with regard to the other queues on this particular cable interface (0 to 10, where 0 is the highest priority and 10 is the lowest priority).
cdxBWQueueNumServedBeforeYield (1.3.6.1.4.1.9.9.116.1.2.1.1.3)	N/A	Maximum number of requests or packets that the scheduler can serve on this queue, before granting access to the next highest-priority queue (0 to 64).

Table B-5 Quality of Service Queues (cdxBWQueueTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxBWQueueType (1.3.6.1.4.1.9.9.116.1.2.1.1.4)	**show interface cable upstream**: Queue ...	Type of queue to be used to decide the position of a request or packet in the queue: unknown(1), other(2), fifo(3), or priority(4).
cdxBWQueueMaxDepth (1.3.6.1.4.1.9.9.116.1.2.1.1.5)	**show interface cable upstream** and **show interface cable mac-scheduler**: Queue ...	Maximum number of requests or packets that this queue can support (0 to 64).
cdxBWQueueDepth (1.3.6.1.4.1.9.9.116.1.2.1.1.6)	**show interface cable upstream** and **show interface cable mac-scheduler**: Queue ...	Number of requests or packets that are currently in this queue (0 to 64).
cdxBWQueueDiscards (1.3.6.1.4.1.9.9.116.1.2.1.1.7)	**show interface cable upstream** and **show interface cable mac-scheduler**: Queue ...	Total number of requests or packets that this queue has discarded because the queue overflowed beyond the maximum specified by cdxBWQueueDepth.

The cdxCmCpeTable in CISCO-DOCS-EXT-MIB contains information about cable modems (CM) or customer premises equipments (CPE) devices. Table B-6 lists the most commonly used objects in this table and the related **show** commands:

Table B-6 Cable Modem and Customer Premises Equipment Information (cdxCmCpeTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxCmCpeMacAddress (1.3.6.1.4.1.9.9.116.1.3.1.1.1)	**show cable device access-group**: MAC address	MAC address of the cable modem or customer premises equipment (CPE) device.
cdxCmCpeType (1.3.6.1.4.1.9.9.116.1.3.1.1.2)	**show cable device access-group**: Type	Type of device: cm(1) or cpe(2).
cdxCmCpeIpAddress (1.3.6.1.4.1.9.9.116.1.3.1.1.3)	**show cable device access-group**: IP address	IP address for this cable modem or customer premises equipment (CPE) device.
cdxCmCpeIfIndex (1.3.6.1.4.1.9.9.116.1.3.1.1.4)	N/A	ifIndex for the cable interface on the CMTS that is connected to this cable modem or customer premises equipment (CPE) device.
cdxCmCpeCmtsServiceId (1.3.6.1.4.1.9.9.116.1.3.1.1.5)	**show interface cable modem**: SID	Primary service ID (SID) for the cable modem itself or for the cable modem that is providing services for this customer premises equipment (CPE) device (1 to 16383).

Table B-6 Cable Modem and Customer Premises Equipment Information (cdxCmCpeTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxCmCpeCmStatusIndex (1.3.6.1.4.1.9.9.116.1.3.1.1.6)	**show interface cable modem**: State	Pointer into the docsIfCmtsCmStatusTable identifying the status of this cable modem or for the cable modem that is providing services for this customer premises equipment (CPE) device (1 to 2147483647).
cdxCmCpeAccessGroup (1.3.6.1.4.1.9.9.116.1.3.1.1.7)	**show cable device access-group**: access-group	ASCII string that identifies the access group to be used to filter the upstream traffic for this cable modem or customer premises equipment (CPE) device.
cdxCmCpeResetNow (1.3.6.1.4.1.9.9.116.1.3.1.1.8)	N/A	Set this object to true(1) to remove a cable modem from the CMTS Station Maintenance list and to force the cable modem to reset its cable interface. If the device is a customer premises equipment (CPE) device, the CMTS removes it from its internal address tables.

The cdxCmtsCmStatusExtTable in CISCO-DOCS-EXT-MIB extends the CM status information in docsIfCmtsCmStatusTable. Table B-7 lists the most commonly used objects in this table and the related **show** commands:

Table B-7 Cable Modem Status Information (cdxCmtsCmStatusExtTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxCmtsCmStatusValue (1.3.6.1.4.1.9.9.116.1.3.2.1.1)	**show cable modem**: MAC State	The cable modem's current connectivity state. This object extends docsIfCmtsCmStatusValue by providing more detailed states.
cdxIfCmtsCmStatusOnlineTimes (1.3.6.1.4.1.9.9.116.1.3.2.1.2)	**show cable modem connectivity**: Times Online	Number of times that this cable modem has changed from the offline state to the online state, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusPercentOnline (1.3.6.1.4.1.9.9.116.1.3.2.1.3)	**show cable modem connectivity**: %online	Percentage of time, in hundredths of a percentage, that this cable modem has remained online, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS (0 to 10000).

Table B-7 Cable Modem Status Information (cdxCmtsCmStatusExtTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxIfCmtsCmStatusMinOnlineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.4)	**show cable modem connectivity**: Online time (min)	Minimum period of time, in hundredths of a second, that this cable modem has remained online, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusAvgOnlineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.5)	**show cable modem connectivity**: Online time (avg)	Average period of time, in hundredths of a second, that this cable modem has remained online, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusMaxOnlineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.6)	**show cable modem connectivity**: Online time (max)	Maximum period of time, in hundredths of a second, that this cable modem has remained online, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusMinOfflineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.7)	**show cable modem connectivity**: Offline time (min)	Minimum period of time, in hundredths of a second, that this cable modem has remained offline, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusAvgOfflineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.8)	**show cable modem connectivity**: Offline time (avg)	Average period of time, in hundredths of a second, that this cable modem has remained offline, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusMaxOfflineTime (1.3.6.1.4.1.9.9.116.1.3.2.1.9)	**show cable modem connectivity**: Offline time (max)	Maximum period of time, in hundredths of a second, that this cable modem has remained offline, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS.
cdxIfCmtsCmStatusDynSidCount (1.3.6.1.4.1.9.9.116.1.3.2.1.10)	N/A	Total number of dynamic service IDs (SIDs) that are active for this cable modem (0 to 16383).
cdxIfCmtsCmStatusAddlInfo (1.3.6.1.4.1.9.9.116.1.3.2.1.11)	N/A	Bit-mask providing additional information about this cable modem: noisyPlant(0) and modemPowerMaxOut(1).

Table B-7 Cable Modem Status Information (cdxCmtsCmStatusExtTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxIfCmtsCmStatusOnlineTimesNum (1.3.6.1.4.1.9.9.116.1.3.2.1.12)	**show cable modem connectivity**: Times Online	Number of times that this cable modem has changed from the offline state to the online state, from the time that the cable modem sent its first Ranging Request (RNG-REQ) message to the CMTS. This object is similar to cdxIfCmtsCmStatusOnlineTimes, but this object is reset to 0 whenever cdxIfCmtsCmStatusLastResetTime is changed.
cdxIfCmtsCmStatusLastResetTime (1.3.6.1.4.1.9.9.116.1.3.2.1.13)	N/A	Time stamp, in terms of sysUpTime, for the last time that the connectivity statistics for this cable modem had been reset.

The cdxIfUpstreamChannelExtTable in CISCO-DOCS-EXT-MIB extends docsIfUpstreamChannelEntry with additional objects that describe the upstream channels. Table B-8 lists the most commonly used objects in this table and the related **show** commands:

Table B-8 Upstream Channel Information (cdxIfUpstreamChannelExtTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-EXT-MIB (ciscoDocsExtMIB)		
cdxIfUpChannelWidth (1.3.6.1.4.1.9.9.116.1.4.1.1.1)	**show interface cable <interface> mac-scheduler <upstream-port>**: Channel width on this upstream channel	Lower frequency, in Hz, for this upstream channel's bandwidth (0 to 16000000). The docsIfUpChannelWidth specifies the higher frequency, and these two objects together specify the upstream channel width to be used for automated advanced spectrum management.
cdxIfUpChannelModulationProfile (1.3.6.1.4.1.9.9.116.1.4.1.1.2)	N/A	Secondary modulation profile to be used for this upstream channel.
cdxIfUpChannelCmTotal (1.3.6.1.4.1.9.9.116.1.4.1.1.3)	**show interface cable <interface> mac-scheduler <upstream-port>**: Total Modems on This Upstream Channel	Total number of cable modems that have been on this upstream channel since the CMTS initially booted (0 to 8191).
cdxIfUpChannelCmActive (1.3.6.1.4.1.9.9.116.1.4.1.1.4)	**show interface cable <interface> mac-scheduler <upstream-port>**: Total Modems on This Upstream Channel	Total number of cable modems that are currently active on this upstream channel (0 to 8191).
cdxIfUpChannelCmRegistered (1.3.6.1.4.1.9.9.116.1.4.1.1.5)	N/A	Total number of cable modems that are currently registered and online on this upstream channel (0 to 8191).
cdxIfUpChannelInputPowerLevel (1.3.6.1.4.1.9.9.116.1.4.1.1.6)	N/A	Upstream input power level, in tenths of a dBmV, for this upstream interface.

Table B-8 Upstream Channel Information (cdxIfUpstreamChannelExtTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
cdxIfUpChannelAvgUtil (1.3.6.1.4.1.9.9.116.1.4.1.1.7)	N/A	Average percentage of the upstream channel's utilization, calculated as the running average of the channel's utilization in the MAC upstream scheduler (0 to 100).
cdxIfUpChannelAvgContSlots (1.3.6.1.4.1.9.9.116.1.4.1.1.8)	N/A	Average percentage of contention mini-slots on this upstream channel, calculated as the running average of contention mini-slots in the MAC upstream scheduler (0 to 100).
cdxIfUpChannelRangeSlots (1.3.6.1.4.1.9.9.116.1.4.1.1.9)	N/A	Average percentage of initial ranging mini-slots on this upstream channel, calculated as the running average of initial ranging mini-slots in the MAC upstream scheduler (0 to 100).
cdxIfUpChannelNumActiveUGS (1.3.6.1.4.1.9.9.116.1.4.1.1.10)	**show interface cable upstream ugs statistics**: # of Active UGS on the Upstream	Number of active unsolicited grant service (UGS) requests on this usptream channel.
cdxIfUpChannelMaxUGSLastOneHour (1.3.6.1.4.1.9.9.116.1.4.1.1.11)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (max)	Maximum number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the previous hour.
cdxIfUpChannelMinUGSLastOneHour (1.3.6.1.4.1.9.9.116.1.4.1.1.12)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (min)	Minimum number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the previous hour.
cdxIfUpChannelAvgUGSLastOneHour (1.3.6.1.4.1.9.9.116.1.4.1.1.13)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (avg)	Average number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the previous hour.
cdxIfUpChannelMaxUGSLastFiveMins (1.3.6.1.4.1.9.9.116.1.4.1.1.14)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (max)	Maximum number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the last five minutes.
cdxIfUpChannelMinUGSLastFiveMins (1.3.6.1.4.1.9.9.116.1.4.1.1.15)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (min)	Minimum number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the last five minutes.
cdxIfUpChannelAvgUGSLastFiveMins (1.3.6.1.4.1.9.9.116.1.4.1.1.16)	**show interface cable upstream ugs statistics**: UGS Allocation Statistics (avg)	Average number of unsolicited grant service (UGS) requests that were allocated on this upstream channel over the last five minutes.

CISCO-DOCS-REMOTE-QUERY

The cdrqCmtsCmStatusTable in CISCO-DOCS-REMOTE-QUERY-MIB contains the status of the cable modems that are polled by the remote-query feature. Table B-9 lists the most commonly used objects in this table and the related **show** commands:

Table B-9 Remote Query Information for Cable Modems (cdrqCmtsCmStatusTable)

Object and OID	Equivalent Show Command and Field	Description
CISCO-DOCS-REMOTE-QUERY (ciscoDocsRemoteQueryMIB)		
cdrqCmtsCmDownChannelPower (1.3.6.1.4.1.9.10.59.1.2.1.1.1)	**show cable modem remote-query**: DS Power	Received power level, in tenths of dBmV, of the cable modem.
cdrqCmtsCmStatusTxPower (1.3.6.1.4.1.9.10.59.1.2.1.1.2)	**show cable modem remote-query**: US Power	Operational transmit power level, in tenths of dBmV, for the cable modem's upstream.
cdrqCmtsCmUpChnlTxTimingOffset (1.3.6.1.4.1.9.10.59.1.2.1.1.3)	**show cable modem remote-query**: TX Time Offset	Latest measure, as a 32-bit unsigned value, for the current round-trip time to the cable modem.
cdrqCmtsCmSigQSignalNoise (1.3.6.1.4.1.9.10.59.1.2.1.1.4)	**show cable modem remote-query**: S/N Ratio	Signal-to-noise ratio (SNR), in tenths of dB, as perceived by the CMTS, for the cable modem's downstream.
cdrqCmtsCmSigQMicroreflections (1.3.6.1.4.1.9.10.59.1.2.1.1.5)	**show cable modem remote-query**: Micro (dB) Reflection	Total microreflections, expressed as dBc below the signal level, as perceived by the CMTS, for the cable modem's downstream.This object is only a rough indication of microflections, including in-channel response, and not an absolute measurement.
cdrqCmtsCmPollTime (1.3.6.1.4.1.9.10.59.1.2.1.1.6)	N/A	Timestamp, in terms of sysUpTime, when this cable modem was last polled by the remote-query feature.

DOCS-IF-MIB

The docsIfSignalQualityTable in DOCS-IF-MIB contains upstream signal information for each ifEntry with an ifType of docsCableUpstreamChannel (205). Table B-10 lists the most commonly used objects in this table and the related **show** commands:

Table B-10 Upstream Signal Information (docsIfSignalQualityTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-IF-MIB (docsIfMib)		
docsIfSigQIncludesContention (1.3.6.1.2.1.10.127.1.1.4.1.1)	**show interface cable signal-quality**: includes contention intervals	Indicates whether the CMTS includes contention intervals in this table's counters. Always false for CMs.
docsIfSigQUnerroreds (1.3.6.1.2.1.10.127.1.1.4.1.2)	N/A	Number of codewords received on this channel without errors.

Table B-10 Upstream Signal Information (docsIfSignalQualityTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsIfSigQCorrecteds (1.3.6.1.2.1.10.127.1.1.4.1.3)	N/A	Number of codewords received on this channel with correctable errors.
docsIfSigQUncorrectables (1.3.6.1.2.1.10.127.1.1.4.1.4)	**show interface cable upstream**: uncorrectable	Number of codewords received on this channel with uncorrectable errors.
docsIfSigQSignalNoise (1.3.6.1.2.1.10.127.1.1.4.1.5)	**show interface cable upstream**: noise	Current signal-to-noise ratio (SNR), in tenths of dB, for this downstream channel (CM) or upstream channel (CMTS).
docsIfSigQMicroreflections (1.3.6.1.2.1.10.127.1.1.4.1.6)	**show interface cable upstream**: microreflections	Rough indication of the total number of microreflections including in-channel response as perceived on this interface, measured in dBc below the signal level (0 to 255).
docsIfSigQEqualizationData (1.3.6.1.2.1.10.127.1.1.4.1.7)	N/A	Equalization data for the downstream channel (CM) or upstream channel (CMTS).

The docsIfCmtsCmStatusTable in DOCS-IF-MIB contains the status information for each CM that is available in the CMTS. Table B-11 lists the most commonly used objects in this table and the related **show** commands:

Table B-11 Cable Modem Status Information (docsIfCmtsCmStatusTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-IF-MIB (docsIfMib)		
docsIfCmtsCmStatusMacAddress (1.3.6.1.2.1.10.127.1.3.3.1.2)	**show cable modem verbose**: MAC Address	MAC address for the CM's cable interface.
docsIfCmtsCmStatusIpAddress (1.3.6.1.2.1.10.127.1.3.3.1.3)	**show cable modem verbose**: IP Address	IP address for the CM's cable interface. This object is deprecated and replaced by docsIfCmtsCmStatusInetAddressType and docsIfCmtsCmStatusInetAddress, to enable migration to IPv6.
docsIfCmtsCmStatusDownChannelIfIndex (1.3.6.1.2.1.10.127.1.3.3.1.4)	**show cable modem verbose**: Interface	ifIndex for the downstream channel being used by this CM.
docsIfCmtsCmStatusUpChannelIfIndex (1.3.6.1.2.1.10.127.1.3.3.1.5)	**show cable modem verbose**: Interface	ifIndex for the upstream channel for this CM.
docsIfCmtsCmStatusRxPower (1.3.6.1.2.1.10.127.1.3.3.1.6)	**show cable modem verbose**: Upstream Power **show cable modem verbose**: Received Power	Receive power level, in tenths of dBmV, for this CM, as perceived by the CMTS on the upstream.
docsIfCmtsCmStatusTimingOffset (1.3.6.1.2.1.10.127.1.3.3.1.7)	**show cable modem verbose**: Timing Offset	Current round-trip time, in 6.25 microseconds/(64*256), for upstream transmissions for this CM.
docsIfCmtsCmStatusEqualizationData (1.3.6.1.2.1.10.127.1.3.3.1.8)	**show cable modem verbose**: Transmit Equalizer Support	Equalization data for this CM.

Table B-11 Cable Modem Status Information (docsIfCmtsCmStatusTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsIfCmtsCmStatusValue (1.3.6.1.2.1.10.127.1.3.3.1.9)	**show cable modem**: MAC State	Current connectivity state for this CM: other(1), ranging(2), rangingAborted(3), rangingComplete(4), ipComplete(5), registrationComplete(6), accessDenied(7).
docsIfCmtsCmStatusUnerroreds (1.3.6.1.2.1.10.127.1.3.3.1.10)	N/A	Number of codewords received without error from this CM. This object is the 32-bit version of docsIfCmtsCmStatusExtUnerroreds, which is a 64-bit counter.
docsIfCmtsCmStatusCorrecteds (1.3.6.1.2.1.10.127.1.3.3.1.11)	N/A	Number of codewords received with correctable errors from this CM. This object is the 32-bit version of docsIfCmtsCmStatusExtCorrecteds, which is a 64-bit counter.
docsIfCmtsCmStatusUncorrectables (1.3.6.1.2.1.10.127.1.3.3.1.12)	N/A	Number of codewords received with uncorrectable errors from this CM. This object is the 32-bit version of docsIfCmtsCmStatusExtUncorrectables, which is a 64-bit counter.
docsIfCmtsCmStatusSignalNoise (1.3.6.1.2.1.10.127.1.3.3.1.13)	N/A	Current signal-to-noise ratio (SNR), in tenths of dB, for this CM, as perceived from its upstream transmissions.
docsIfCmtsCmStatusMicroreflections (1.3.6.1.2.1.10.127.1.3.3.1.14)	N/A	Rough indication of the total number of microreflections, including in-channel response, perceived for this CM, as measured in dBc below the signal level.
docsIfCmtsCmStatusExtUnerroreds (1.3.6.1.2.1.10.127.1.3.3.1.15)	N/A	Number of codewords received without error from this CM. This object is the 64-bit version of docsIfCmtsCmStatusUnerroreds, which is a 32-bit counter.
docsIfCmtsCmStatusExtCorrecteds (1.3.6.1.2.1.10.127.1.3.3.1.16)	N/A	Number of codewords received with correctable errors from this CM. This object is the 64-bit version of docsIfCmtsCmStatusCorrecteds, which is a 32-bit counter.
docsIfCmtsCmStatusExtUncorrectables (1.3.6.1.2.1.10.127.1.3.3.1.17)	N/A	Number of codewords received with uncorrectable errors from this CM. This object is the 64-bit version of docsIfCmtsCmStatusUncorrectables, which is a 32-bit counter.

Table B-11 Cable Modem Status Information (docsIfCmtsCmStatusTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsIfCmtsCmStatusDocsisRegMode (1.3.6.1.2.1.10.127.1.3.3.1.18)	**show cable modem verbose**: QoS Provisioned Mode	Indicates the DOCSIS QoS revision level at which this CM is currently registered. This object replaces docsIfCmtsCmStatusDocsisMode from DOCS-IF-EXT-MIB.
docsIfCmtsCmStatusModulationType (1.3.6.1.2.1.10.127.1.3.3.1.19)	**show cable modem verbose**: Phy Operating Mode	Indicates the upstream PHY mode (TDMA, A-TDMA, S-CDMA) that the CM is registered for and currently using. (The mixed TDMA/A-TDMA mode is not supported here, because that describes the upstream interface and not the behavior of individual CMs.)
docsIfCmtsCmStatusInetAddressType (1.3.6.1.2.1.10.127.1.3.3.1.20)	**show cable modem verbose**: IP Address	Type of IP address that this CM is using (IPv4 or IPv6).
docsIfCmtsCmStatusInetAddress (1.3.6.1.2.1.10.127.1.3.3.1.21)	**show cable modem verbose**: IP Address	IP address for this CM's cable interface. This object, together with docsIfCmtsCmStatusInetAddressType, replace docsIfCmtsCmStatusIpAddress.

The docsIfCmtsModulationTable in DOCS-IF-MIB describes an Interval Usage Code (IUC) for one or more upstream channel modulation profiles. Table B-12 lists the most commonly used objects in this table and the related **show** commands:

Table B-12 Interval Usage Code Upstream Configuration (docsIfCmtsModulationTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-IF-MIB (docsIfMib)		
docsIfCmtsModIntervalUsageCode (1.3.6.1.2.1.10.127.1.3.5.1.2)	**show cable modulation-profile** [**verbose**]: IUC, IUC	Type of IUC being defined: request(1), requestData(2), initialRanging(3), periodicRanging(4), shortData(5), longData(6), dvPhyShortData(9), advPhyLongData(10), and ugs(11).
docsIfCmtsModType (1.3.6.1.2.1.10.127.1.3.5.1.4)	**show cable modulation-profile** [**verbose**]: Type, Modulation	Modulation type for this burst profile: QPSK, 8-QAM, 16-QAM, 32-QAM, 64-QAM, and 128-QAM.
docsIfCmtsModPreambleLen (1.3.6.1.2.1.10.127.1.3.5.1.5)	**show cable modulation-profile** [**verbose**]: Pre len, Preamble length	Preamble length, in bits, for this burst profile (0 to 1536 bits).
docsIfCmtsModDifferentialEncoding (1.3.6.1.2.1.10.127.1.3.5.1.6)	**show cable modulation-profile** [**verbose**]: Diff enco, Differential Encoding	Specifies whether differential encoding is enabled on this burst profile.
docsIfCmtsModFECErrorCorrection (1.3.6.1.2.1.10.127.1.3.5.1.7)	**show cable modulation-profile** [**verbose**]: FEC T BYTE, FEC parity T bytes	Number of correctable errored bytes (t) that should be used for forward error correction (FEC) on this burst profile (0 to 16).

Table B-12 Interval Usage Code Upstream Configuration (docsIfCmtsModulationTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsIfCmtsModFECCodewordLength (1.3.6.1.2.1.10.127.1.3.5.1.8)	**show cable modulation-profile** [**verbose**]: FEC k BYTE, FEC codeword length K bytes	Number of data bytes (k) in each FEC codeword (1 to 255).
docsIfCmtsModScramblerSeed (1.3.6.1.2.1.10.127.1.3.5.1.9)	**show cable modulation-profile** [**verbose**]: Scrmb seed, Scrambler seed	Fifteen-bit seed value for the scrambler used on this burst profile (0 to 32767).
docsIfCmtsModMaxBurstSize (1.3.6.1.2.1.10.127.1.3.5.1.10)	**show cable modulation-profile** [**verbose**]: Max B siz, Max short busrt size B bytes	Maximum number of mini-slots that can be transmitted during this particular burst (0 to 255).
docsIfCmtsModGuardTimeSize (1.3.6.1.2.1.10.127.1.3.5.1.11)	**show cable modulation-profile** [**verbose**]: Guard time size, Guard time size in symbols	Number of symbol-times that are appended to this particular burst as a guard time.
docsIfCmtsModLastCodewordShortened (1.3.6.1.2.1.10.127.1.3.5.1.12)	**show cable modulation-profile** [**verbose**]: Last CW short, Shortened last codeword	Indicates whether the last FEC codeword is truncated.
docsIfCmtsModScrambler (1.3.6.1.2.1.10.127.1.3.5.1.13)	**show cable modulation-profile** [**verbose**]: Scrmb, Scrambler	Indicates whether the scrambler is enabled for this burst profile.
docsIfCmtsModByteInterleaverDepth (1.3.6.1.2.1.10.127.1.3.5.1.14)	**show cable modulation-profile** [**verbose**]: RS interleaver depth	A-TDMA byte interleaver depth (Ir).
docsIfCmtsModByteInterleaverBlockSize (1.3.6.1.2.1.10.127.1.3.5.1.15)	**show cable modulation-profile** [**verbose**]: RS interleaver block size	A-TDMA byte interleaver block size (Br).
docsIfCmtsModPreambleType (1.3.6.1.2.1.10.127.1.3.5.1.16)	**show cable modulation-profile** [**verbose**]: Pre Type, Preamble type	Preamble type for DOCSIS 2.0 burst profiles: qpsk0(1), qpsk1(2).
docsIfCmtsModTcmErrorCorrectionOn (1.3.6.1.2.1.10.127.1.3.5.1.17)	N/A	Indicates whether trellis code modulation (TCM) is enabled for S-CDMA burst profiles.
docsIfCmtsModScdmaInterleaverStepSize (1.3.6.1.2.1.10.127.1.3.5.1.18)	N/A	Interleaver step size for S-CDMA burst profiles (0, 1 to 32).
docsIfCmtsModScdmaSpreaderEnable (1.3.6.1.2.1.10.127.1.3.5.1.19)	N/A	Indicates whether the spreader is enabled for S-CDMA burst profiles.
docsIfCmtsModScdmaSubframeCodes (1.3.6.1.2.1.10.127.1.3.5.1.20)	N/A	Subframe size for S-CDMA burst profiles (0, 1 to 128).
docsIfCmtsModChannelType (1.3.6.1.2.1.10.127.1.3.5.1.21)	N/A	Modulation channel type for this burst profile: tdma (1), atdma (2), scdma (3), and tdmaAndAtdma (4).

DOCS-QOS-MIB

The docsQosPktTable in DOCS-QOS-MIB describes the packet classification configured on the Cisco CMTS router. Table B-13 lists the most commonly used objects in this table and the related **show** commands:

Table B-13 DOCSIS Packet Classifiers (docsQosPktTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosPktClassId (1.3.6.1.2.1.10.127.7.1.1.1.1)	**show cable modem classifiers**: CfrId	ID for this packet classifier entry (1 to 65535).
docsQosPktClassDirection (1.3.6.1.2.1.10.127.7.1.1.1.2)	**show cable modem classifiers**: Direction	Indicates the direction (upstream or downstream) in which this classifier is applied.
docsQosPktClassPriority (1.3.6.1.2.1.10.127.7.1.1.1.3)	**show cable modem classifiers**: Priority	Priority for this classifier, which determines the order in which the classifiers are evaluated (0 to 255).
docsQosPktClassIpTosLow (1.3.6.1.2.1.10.127.7.1.1.1.4)	**show cable modem classifiers cache**: ToS	Low 8 bits for the range of type of service (ToS) values to be matched (0 to 255).
docsQosPktClassIpTosHigh (1.3.6.1.2.1.10.127.7.1.1.1.5)	**show cable modem classifiers cache**: ToS	High 8 bits for the range of type of service (ToS) values to be matched (0 to 255).
docsQosPktClassIpTosMask (1.3.6.1.2.1.10.127.7.1.1.1.6)	**show cable modem classifiers cache**: ToS	And Mask value for the ToS bytes in an IP packet, and the result is checked against the low and high ToS byte values.
docsQosPktClassIpProtocol (1.3.6.1.2.1.10.127.7.1.1.1.7)	**show cable modem classifiers cache**: IPProt	IP Layer-4 protocol field to be matched against packets (0 to 258, where 256 matches all protocols, and 257 matches both TCP and UDP).
docsQosPktClassIpSourceAddr (1.3.6.1.2.1.10.127.7.1.1.1.8)	**show cable modem classifiers cache**: IpSrc	Source IP address to be matched.
docsQosPktClassIpSourceMask (1.3.6.1.2.1.10.127.7.1.1.1.9)	N/A	Source IP address mask to be matched.
docsQosPktClassIpDestAddr (1.3.6.1.2.1.10.127.7.1.1.1.10)	**show cable modem classifiers cache**: IpDest	Destination IP address to be matched.
docsQosPktClassIpDestMask (1.3.6.1.2.1.10.127.7.1.1.1.11)	N/A	Destination IP address mask to be matched.
docsQosPktClassSourcePortStart (1.3.6.1.2.1.10.127.7.1.1.1.12)	N/A	Low value of the range of source TCP/UDP port numbers to be matched (0 to 65535).

Table B-13 DOCSIS Packet Classifiers (docsQosPktTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosPktClassSourcePortEnd (1.3.6.1.2.1.10.127.7.1.1.1.13)	N/A	High value of the range of source TCP/UDP port numbers to be matched (0 to 65535).
docsQosPktClassDestPortStart (1.3.6.1.2.1.10.127.7.1.1.1.14)	N/A	Low value of the range of destination TCP/UDP port numbers to be matched (0 to 65535).
docsQosPktClassDestPortEnd (1.3.6.1.2.1.10.127.7.1.1.1.15)	N/A	High value of the range of destination TCP/UDP port numbers to be matched (0 to 65535).
docsQosPktClassDestMacAddr (1.3.6.1.2.1.10.127.7.1.1.1.16)	N/A	Destination MAC address to be matched.
docsQosPktClassDestMacMask (1.3.6.1.2.1.10.127.7.1.1.1.17)	N/A	Destination MAC address mask to be matched.
docsQosPktClassSourceMacAddr (1.3.6.1.2.1.10.127.7.1.1.1.18)	N/A	Source MAC address to be matched.
docsQosPktClassEnetProtocolType (1.3.6.1.2.1.10.127.7.1.1.1.19)	N/A	Layer 3 protocol ID in the Ethernet frame that should be matched (0 to 65535).
docsQosPktClassEnetProtocol (1.3.6.1.2.1.10.127.7.1.1.1.20)	N/A	Ethernet Type value to be matched (0 to 65535).
docsQosPktClassUserPriLow (1.3.6.1.2.1.10.127.7.1.1.1.22)	N/A	Indicates the low value of the range of 3-bit priority fields to be matched, for Ethernet frames with an EtherType of 0x8100 and an 802.1P/Q tag header (0 to 7).
docsQosPktClassUserPriHigh (1.3.6.1.2.1.10.127.7.1.1.1.23)	N/A	Indicates the high value of the range of 3-bit priority fields to be matched, for Ethernet frames with an EtherType of 0x8100 and an 802.1P/Q tag header (0 to 7).
docsQosPktClassVlanId (1.3.6.1.2.1.10.127.7.1.1.1.24)	N/A	Indicates the 12-bit VLAN ID to be matched, for Ethernet frames with an EtherType of 0x8100 and an 802.1P/Q tag header (0 to 7).
docsQosPktClassState (1.3.6.1.2.1.10.127.7.1.1.1.25)	N/A	Indicates whether the classifier is active(1) or inactive(2).
docsQosPktClassPkts (1.3.6.1.2.1.10.127.7.1.1.1.26)	N/A	Number of packets that have been classified using this classifier.
docsQosPktClassBitMap (1.3.6.1.2.1.10.127.7.1.1.1.27)	N/A	17-bit bitmask that indicates the parameter encodings that were actually present in the DOCSIS message that created the classifier, as opposed to parameters that were unspecified and left at their default values.

The docsQosParamSetTable in DOCS-QOS-MIB describes the DOCSIS 1.1 QoS parameters that are defined on the Cisco CMTS router. Table B-14 lists the most commonly used objects in this table and the related **show** commands:

Table B-14 DOCSIS 1.1 Quality of Service Parameters (docsQosParamSetTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosParamSetServiceClassName (1.3.6.1.2.1.10.127.7.1.2.2.4)	**show cable service-class verbose**: Name **show interface cable qos paramset verbose**: Name	Service class name (SCN) for this parameter set.
docsQosParamSetPriority (1.3.6.1.2.1.10.127.7.1.2.2.5)	**show cable service-class verbose**: Traffic Priority **show interface cable qos paramset verbose**: Traffic Priority	Relative priority for this service flow (0 to 7), which determines the priority of service flows that have identical parameter sets.
docsQosParamSetMaxTrafficRate (1.3.6.1.2.1.10.127.7.1.2.2.6)	**show cable service-class verbose**: Maximum Sustained Rate **show interface cable qos paramset verbose**: Maximum Sustained Rate	Maximum sustained traffic rate, in bits per second, for this service flow.
docsQosParamSetMaxTrafficBurst (1.3.6.1.2.1.10.127.7.1.2.2.7)	**show cable service-class verbose**: Max Burst **show interface cable qos paramset verbose**: Max Burst	Token bucket size, in bytes, for this parameter set.
docsQosParamSetMinReservedRate (1.3.6.1.2.1.10.127.7.1.2.2.8)	**show cable service-class verbose**: Minimum Reserved Rate **show interface cable qos paramset verbose**: Minimum Reserved Rate	Guaranteed minimum rate, in bits per second, for this parameter set.
docsQosParamSetMinReservedPkt (1.3.6.1.2.1.10.127.7.1.2.2.9)	**show cable service-class verbose**: Minimum Packet Size **show interface cable qos paramset verbose**: Minimum Packet Size	Minimum packet size, in bytes, for which the docsQosParamSetMinReservedRate is provided (0 to 65535).
docsQosParamSetActiveTimeout (1.3.6.1.2.1.10.127.7.1.2.2.10)	**show cable service-class verbose**: Active QoS Timeout **show interface cable qos paramset verbose**: Active QoS Timeout	Maximum time, in seconds, that resources can remain unused while in the active state being being released (0 to 65535, where 0 indicates no timeout).

Table B-14 DOCSIS 1.1 Quality of Service Parameters (docsQosParamSetTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosParamSetAdmittedTimeout (1.3.6.1.2.1.10.127.7.1.2.2.11)	**show cable service-class verbose**: Admitted QoS Timeout **show interface cable qos paramset verbose**: Admitted QoS Timeout	Maximum time, in seconds, that resources can remain in the admitted state before being released (0 to 65535, where 0 indicates no timeout).
docsQosParamSetMaxConcatBurst (1.3.6.1.2.1.10.127.7.1.2.2.12)	**show interface cable qos paramset verbose**: Maximum Concatenated Burst	Maximum size of the concatenated burst, in bytes, that is allowed on this upstream (0 to 65535).
docsQosParamSetSchedulingType (1.3.6.1.2.1.10.127.7.1.2.2.13)	**show cable service-class verbose**: Scheduling Type **show interface cable qos paramset verbose**: Scheduling Type	Upstream scheduling type that is used for this upstream service flow.
docsQosParamSetNomPollInterval (1.3.6.1.2.1.10.127.7.1.2.2.15)	N/A	Interval, in microseconds, between successive unicast request opportunities on the upstream service flow.
docsQosParamSetTolPollJitter (1.3.6.1.2.1.10.127.7.1.2.2.16)	N/A	Maximum amount of time, in microseconds, that unicast request intervals can be delayed from the regularly scheduled times on an usptream service flow.
docsQosParamSetUnsolicitGrantSize (1.3.6.1.2.1.10.127.7.1.2.2.17)	**show cable service-class verbose**: Unsolicited Grant Size	Unsolicited grant size, in bytes (0 to 65535) for UGS and UGS-AD service flows.
docsQosParamSetNomGrantInterval (1.3.6.1.2.1.10.127.7.1.2.2.18)	**show cable service-class verbose**: Nominal Grant Interval	Nominal time, in microseconds, between successive data grant opportunities on an upstream service flow.
docsQosParamSetTolGrantJitter (1.3.6.1.2.1.10.127.7.1.2.2.19)	**show cable service-class verbose**: Tolerated Grant Jitter	Maximum amount of time, in microseconds, that the transmission opportunities might be delayed from the regularly scheduled times for UGS and UGS-AD service flows.
docsQosParamSetGrantsPerInterval (1.3.6.1.2.1.10.127.7.1.2.2.20)	**show cable service-class verbose**: Grants per Interval	Number of data grants allowed per grant interval (0 to 127).
docsQosParamSetTosAndMask (1.3.6.1.2.1.10.127.7.1.2.2.21)	**show cable service-class verbose**: IP ToS Overwrite [AND-mask, OR-mask] **show interface cable qos paramset verbose**: IP ToS Overwrite [AND-mask, OR-mask]	AND mask for the IP type of service (ToS) byte.

Table B-14 DOCSIS 1.1 Quality of Service Parameters (docsQosParamSetTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosParamSetTosOrMask (1.3.6.1.2.1.10.127.7.1.2.2.22)	**show cable service-class verbose**: IP ToS Overwrite [AND-mask, OR-mask] **show interface cable qos paramset verbose**: IP ToS Overwrite [AND-mask, OR-mask]	OR mask for the IP Type of Service (ToS) byte.
docsQosParamSetMaxLatency (1.3.6.1.2.1.10.127.7.1.2.2.23)	**show cable service-class verbose**: Max Latency	Maximum latency, in microseconds, between the time the CMTS receives a packet on its network-side interface (NSI) and forwards it on the RF cable interface.
docsQosParamSetType (1.3.6.1.2.1.10.127.7.1.2.2.24)	N/A	Indicates the type for this QoS parameter set: active(1), admitted(2), and provisioned(3).
docsQosParamSetRequestPolicyOct (1.3.6.1.2.1.10.127.7.1.2.2.25)	**show cable service-class verbose**: Request/Transmission Policy **show interface cable qos paramset verbose**: Request/Transmission Policy	32-bit bitmask that specifies the transmit interval opportunities that the CM omits for upstream transmission requests and packet transmissions. This object replaces docsQosParamSetRequestPolicy.
docsQosParamSetBitMap (1.3.6.1.2.1.10.127.7.1.2.2.26)	**show cable service-class verbose**: Parameter Presence Bitfield **show interface cable qos paramset verbose**: Parameter Presence Bitfield	Bitmask that indicates the set of parameters actually included in the DOCSIS registration or dynamic service request message that created the parameter set.

The docsQosServiceFlowIdTable in DOCS-QOS-MIB extends the information about a service ID (SID) in docsIfCmtsServiceTable. Table B-15 lists the most commonly used objects in this table and the related **show** commands:

Table B-15 Service ID Information (docsQosServiceFlowIdTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosServiceFlowId (1.3.6.1.2.1.10.127.7.1.3.1.1)	**show interface cable service-flow**: Sfid	Service flow ID (SFID) assigned to this service flow (1 to 4294967295).
docsQosServiceFlowSID (1.3.6.1.2.1.10.127.7.1.3.1.6)	**show interface cable service-flow**: Sid	Service ID (SID) that is assigned to an admitted or active service flow (0 to 16383). Provisioned service flows are not assigned a SID.
docsQosServiceFlowDirection (1.3.6.1.2.1.10.127.7.1.3.1.7)	**show interface cable service-flow**: Dir	Direction of the service flow (upstream or downstream).
docsQosServiceFlowPrimary (1.3.6.1.2.1.10.127.7.1.3.1.8)	**show interface cable service-flow**: Type	Indicates whether the service flow is the primary flow or a secondary flow.

The docsQosServiceFlowStatsTable in DOCS-QOS-MIB contains service flow statistics. Table B-16 lists the most commonly used objects in this table and the related **show** commands:

Table B-16 Service Flow Statistics (docsQosServiceFlowStatsTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosServiceFlowPkts (1.3.6.1.2.1.10.127.7.1.4.1.1)	**show interface cable service-flow counters verbose**: Packets	Number of packets sent using this service flow.
docsQosServiceFlowOctets (1.3.6.1.2.1.10.127.7.1.4.1.2)	**show interface cable service-flow counters verbose**: Octets	Number of octets sent using this service flow, after payload header suppression (PHS) has been applied.
docsQosServiceFlowTimeCreated (1.3.6.1.2.1.10.127.7.1.4.1.3)	N/A	Time stamp, in terms of sysUpTime, for when this service flow was created.
docsQosServiceFlowTimeActive (1.3.6.1.2.1.10.127.7.1.4.1.4)	**show interface cable service-flow**: Active Time	Total time, in seconds, this service flow has been active.
docsQosServiceFlowPHSUnknowns (1.3.6.1.2.1.10.127.7.1.4.1.5)	N/A	Number of packets that had an unknown payload header suppression index.
docsQosServiceFlowPolicedDropPkts (1.3.6.1.2.1.10.127.7.1.4.1.6)	**show interface cable service-flow counters verbose**: RateLimit Dropped Pkts	Number of packets sent using this service flow that were dropped due to a violation of the flow's policies, especially because they would have exceeded the maximum traffic rate.
docsQosServiceFlowPolicedDelayPkts (1.3.6.1.2.1.10.127.7.1.4.1.7)	**show interface cable service-flow counters verbose**: RateLimit Delayed Pkts	Number of packets sent using this service flow that were delayed because of the flow's policies, especially because they would have otherwise exceeded the maximum traffic rate.

The docsQosUpstreamStatsTable in DOCS-QOS-MIB provides upstream service flow statistics. Table B-17 lists the most commonly used objects in this table and the related **show** commands:

Table B-17 Upstream Service Flow Statistics (docsQosUpstreamStatsTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosSID (1.3.6.1.2.1.10.127.7.1.5.1.1)	**show interface cable sid counters verbose**: Sid	Service ID (SID) for an admitted or active upstream service flow (1 to 16383).
docsQosUpstreamFragments (1.3.6.1.2.1.10.127.7.1.5.1.2)	N/A	Number of fragmentation headers that were received on an upstream service flow.

Table B-17 Upstream Service Flow Statistics (docsQosUpstreamStatsTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosUpstreamFragDiscards (1.3.6.1.2.1.10.127.7.1.5.1.3)	N/A	Number of upstream fragments that were discarded and not reassembled into a complete packet.
docsQosUpstreamConcatBursts (1.3.6.1.2.1.10.127.7.1.5.1.4)	N/A	Number of concatenation headers received on an upstream service flow.

The docsQosServiceClassTable in DOCS-QOS-MIB describes the DOCSIS service classes on a CMTS. Table B-18 lists the most commonly used objects in this table and the related **show** commands:

Table B-18 DOCSIS Service Classes (docsQosServiceClassTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosServiceClassName (1.3.6.1.2.1.10.127.7.1.8.1.1)	**show cable service-class** [**verbose**]: Name **show interface cable qos paramset verbose**: Name	Unique name of the service class (up to 15 ASCII characters in length).
docsQosServiceClassPriority (1.3.6.1.2.1.10.127.7.1.8.1.4)	**show cable service-class** [**verbose**]: Prio, Traffic Priority **show interface cable qos paramset verbose**: Traffic Priority	Priority value (0 to 7) to be used for docsQosParamSetPriority.
docsQosServiceClassMaxTrafficRate (1.3.6.1.2.1.10.127.7.1.8.1.5)	**show cable service-class** [**verbose**]: MaxSusRate, Maximum Sustained Rate **show interface cable qos paramset verbose**: Maximum Sustained Rate	Maximum bit rate (in bps) for the docsQosParamSetMaxTrafficRate.
docsQosServiceClassMaxTrafficBurst (1.3.6.1.2.1.10.127.7.1.8.1.6)	**show cable service-class** [**verbose**]: MaxBurst, Max Burst **show interface cable qos paramset verbose**: Max Burst	Maximum number of bytes for the docsQosParamSetMaxTrafficBurst.
docsQosServiceClassMinReservedRate (1.3.6.1.2.1.10.127.7.1.8.1.7)	**show cable service-class** [**verbose**]: MinRsvRate, Minimum Reserved Rate **show interface cable qos paramset verbose**: Minimum Reserved Rate	Minimum bit rate (in bps) for the minimum guaranteed service rate (docsQosParamSEtMinReservedRate).

Table B-18 DOCSIS Service Classes (docsQosServiceClassTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosServiceClassMinReservedPkt (1.3.6.1.2.1.10.127.7.1.8.1.8)	**show cable service-class verbose**: Minimum Packet Size **show interface cable qos paramset verbose**: Minimum Packet Size	Minimum packet size, in bytes, for for docsQosParamSetMinReservedPkt (0 to 65535).
docsQosServiceClassMaxConcatBurst (1.3.6.1.2.1.10.127.7.1.8.1.9)	**show interface cable qos paramset verbose**: Maximum Concatenated Burst	Maximum size of the concatenated burst, in bytes, that is allowed on this upstream (0 to 65535), for docsQosParamSetMaxConcatBurst.
docsQosServiceClassNomPollInterval (1.3.6.1.2.1.10.127.7.1.8.1.10)	N/A	Interval, in microseconds, between successive unicast request opportunities on the upstream service flow (docsQosParamSetNomPollInterval.)
docsQosServiceClassTolPollJitter (1.3.6.1.2.1.10.127.7.1.8.1.11)	N/A	Maximum amount of time, in microseconds, that unicast request intervals can be delayed from the regularly scheduled times on an usptream service flow (docsQosParamSetTolPollJitter).
docsQosServiceClassUnsolicitGrantSize (1.3.6.1.2.1.10.127.7.1.8.1.12)	**show cable service-class verbose**: Unsolicited Grant Size	Unsolicited grant size, in bytes (0 to 65535) for UGS and UGS-AD service flows (docsQosParamSetUnsolicitGrantSize).
docsQosServiceClassNomGrantInterval (1.3.6.1.2.1.10.127.7.1.8.1.13)	**show cable service-class verbose**: Nominal Grant Interval	Nominal time, in microseconds, between successive data grant opportunities on an upstream service flow (docsQosParamSetNomGrantInterval).
docsQosServiceClassTolGrantJitter (1.3.6.1.2.1.10.127.7.1.8.1.14)	**show cable service-class verbose**: Tolerated Grant Jitter	Maximum amount of time, in microseconds, that the transmission opportunities might be delayed from the regularly scheduled times for UGS and UGS-AD service flows (docsQosParamSetTolGrantJitter).
docsQosServiceClassGrantsPerInterval (1.3.6.1.2.1.10.127.7.1.8.1.15)	**show cable service-class verbose**: Grants per Interval	Number of data grants allowed per grant interval (0 to 127) for docsQosParamSetGrantsPerInterval.
docsQosServiceClassMaxLatency (1.3.6.1.2.1.10.127.7.1.8.1.16)	**show cable service-class verbose**: Max Latency	Maximum latency, in microseconds, between the time the CMTS receives a packet on its network-side interface (NSI) and forwards it on the RF cable interface, for docsQosParamSetClassMaxLatency.
docsQosServiceClassActiveTimeout (1.3.6.1.2.1.10.127.7.1.8.1.17)	**show interface cable qos paramset verbose**: Active QoS Timeout	Maximum time, in seconds, that resources can remain unused while in the active state being being released (0 to 65535, where 0 indicates no timeout), for docsQosServiceFlowActiveTimeout.

Table B-18 DOCSIS Service Classes (docsQosServiceClassTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsQosServiceClassAdmittedTimeout (1.3.6.1.2.1.10.127.7.1.8.1.18)	**show interface cable qos paramset verbose**: Admitted QoS Timeout	Maximum time, in seconds, that resources can remain in the admitted state before being released (0 to 65535, where 0 indicates no timeout), for docsQosServiceFlowAdmittedTimeout.
docsQosServiceClassSchedulingType (1.3.6.1.2.1.10.127.7.1.8.1.19)	**show cable service-class** [**verbose**]: Sched, Scheduling Type **show interface cable qos paramset verbose**: Scheduling Type	Upstream scheduling type that is used for this upstream service flow, for docsQosServiceFlowSchedulingType.
docsQosServiceClassRequestPolicy (1.3.6.1.2.1.10.127.7.1.8.1.20)	**show cable service-class verbose**: Request/Transmission Policy **show interface cable qos paramset verbose**: Request/Transmission Policy	32-bit bitmask that specifies the transmit interval opportunities that the CM omits for upstream transmission requests and packet transmissions, for docsQosServiceFlowRequestPolicy.
docsQosServiceClassTosAndMask (1.3.6.1.2.1.10.127.7.1.8.1.21)	**show cable service-class verbose**: IP Tos Overwrite [AND-mask, OR-mask] **show interface cable qos paramset verbose**: IP ToS Overwrite [AND-mask, OR-mask]	AND mask for the IP Type of Service (ToS) byte, for docsQosServiceFlowTosAndMask.
docsQosServiceClassTosOrMask (1.3.6.1.2.1.10.127.7.1.8.1.22)	**show cable service-class verbose**: IP Tos Overwrite [AND-mask, OR-mask] **show interface cable qos paramset verbose**: IP ToS Overwrite [AND-mask, OR-mask]	OR mask for the IP Type of Service (ToS) byte, for docsQosServiceFlowTosOrMask.
docsQosServiceClassDirection (1.3.6.1.2.1.10.127.7.1.8.1.23)	**show cable service-class** [**verbose**]: Dir, Direction **show interface cable qos paramset verbose**: Direction	Direction for this service class template (upstream or downstream).

The docsQosPHSTable in DOCS-QOS-MIB describes the payload header suppression (PHS) rules that are configured on the Cisco CMTS router. Table B-19 lists the most commonly used objects in this table and the related **show** commands:

Table B-19 Payload Header Suppression Rules (docsQosPHSTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-QOS-MIB (docsQosMib)		
docsQosPHSField (1.3.6.1.2.1.10.127.7.1.10.1.2)	**show interface cable service-flow phs verbose**: PHSF	8-bit value that defines the header bytes that should be suppressed.
docsQosPHSMask (1.3.6.1.2.1.10.127.7.1.10.1.3)	**show interface cable service-flow phs verbose**: PHSM	5-bit PHS mask that defines the header bytes that should be suppressed.
docsQosPHSSize (1.3.6.1.2.1.10.127.7.1.10.1.4)	**show interface cable service-flow phs verbose**: PHSS	8-bit value specifying the number of header bytes to be suppressed.
docsQosPHSVerify (1.3.6.1.2.1.10.127.7.1.10.1.5)	**show interface cable service-flow phs verbose**: PHSV	Indicates whether PHS verification is enabled.
docsQosPHSIndex (1.3.6.1.2.1.10.127.7.1.10.1.7)	**show interface cable service-flow phs verbose**: PHSI	Index that uniquely references the PHS rule.

DOCS-SUBSCRIBER-MIB

The docsSubMgtPktFilterTable in DOCS-SUBSCRIBER-MIB is a generic packet filter table that is linked to specific cable modems through the linked by the docsSubMgtCmFilterTable. Table B-20 lists the most commonly used objects in this table and the related **show** commands:

Table B-20 Generic Packet Filter Table (docsSubMgtPktFilterTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-SUBSCRIBER-MIB (docsSubMgt)		
docsSubMgtPktFilterGroup (1.3.6.1.3.83.4.1.6.1.1)	**show cable filter** [**verbose**]: Filter Grp, Filter Group	Identifies this specific group of filters (1 to 1024).
docsSubMgtPktFilterIndex (1.3.6.1.3.83.4.1.6.1.2)	**show cable filter** [**verbose**]: Filter Id, Filter index	Index that describes the order in which filter groups are applied (1 to 1024).
docsSubMgtPktFilterSrcAddr (1.3.6.1.3.83.4.1.6.1.3)	**show cable filter** [**verbose**]: SrcAddr/Mask, Source IP Address	Source IP address to be matched.
docsSubMgtPktFilterSrcMask (1.3.6.1.3.83.4.1.6.1.4)	**show cable filter** [**verbose**]: SrcAddr/Mask, Source IP Address	Source IP address mask to be matched.
docsSubMgtPktFilterDstAddr (1.3.6.1.3.83.4.1.6.1.5)	**show cable filter** [**verbose**]: DestAddr/Mask, Destination IP Address	Destination IP address to be matched.

Table B-20 Generic Packet Filter Table (docsSubMgtPktFilterTable) (continued)

Object and OID	Equivalent Show Command and Field	Description
docsSubMgtPktFilterDstMask (1.3.6.1.3.83.4.1.6.1.6)	**show cable filter** [**verbose**]: DestAddr/Mask, Destination IP Address	Destination IP address mask to be matched.
docsSubMgtPktFilterUlp (1.3.6.1.3.83.4.1.6.1.7)	**show cable filter** [**verbose**]: Prot, IP Protocol type	Number of the upper level (Layer 4 and above) protocol to be matched (0 to 256, where 6 indicates TCP, 17 indicates UDP, and 256 matches anything).
docsSubMgtPktFilterTosValue (1.3.6.1.3.83.4.1.6.1.8)	**show cable filter** [**verbose**]: ToS, IP ToS (Mask, Value)	IP type of service (TOS) value to be matched (0 to 7).
docsSubMgtPktFilterTosMask (1.3.6.1.3.83.4.1.6.1.9)	**show cable filter** [**verbose**]: ToS, IP ToS (Mask, Value)	IP type of service (TOS) mask to be matched (0 to 7).
docsSubMgtPktFilterAction (1.3.6.1.3.83.4.1.6.1.10)	**show cable filter** [**verbose**]: Action, Match action	Action to be taken when a packet is matched: accept(1) or drop(2).
docsSubMgtPktFilterMatches (1.3.6.1.3.83.4.1.6.1.11)	**show cable filter verbose**: Matches	Number of times this specific filter rule has been matched, which occurs only when all components of the filter are matched against a packet. If a packet might match multiple filters, this counter is incremented only on the first filter that is matched.

The docsSubMgtTcpUdpFilterTable in DOCS-SUBSCRIBER-MIB extends the docsSubMgtPktFilterTable to provide optional filtering based on elements in TCP or UDP headers. Table B-21 lists the most commonly used objects in this table and the related **show** commands:

Table B-21 TCP and UDP Header Filters (docsSubMgtTcpUdpFilterTable)

Object and OID	Equivalent Show Command and Field	Description
DOCS-SUBSCRIBER-MIB (docsSubMgt)		
docsSubMgtTcpUdpSrcPort (1.3.6.1.3.83.4.1.7.1.1)	**show cable filter** [**verbose**]: SPort, TCP/UDP Source Port	Source TCP/UDP port to be matched (0 to 65536, where 65536 matches any value).
docsSubMgtTcpUdpDstPort (1.3.6.1.3.83.4.1.7.1.2)	**show cable filter** [**verbose**]: DPort, TCP/UDP Destination Port	Destination TCP/UDP port to be matched (0 to 65536, where 65536 matches any value).
docsSubMgtTcpFlagValues (1.3.6.1.3.83.4.1.7.1.3)	**show cable filter** [**verbose**]: TCP flags, TCP Flags (mask, value)	Bit-mask containing the TCP flag values to be matched: urgent(0), ack(1), push(2), reset(3), syn(4), and fin(5).
docsSubMgtTcpFlagMask (1.3.6.1.3.83.4.1.7.1.4)	**show cable filter** [**verbose**]: TCP flags, TCP Flags (mask, value)	Bit-mask containing mask for bits to be checked for matching: urgent(0), ack(1), push(2), reset(3), syn(4), and fin(5).

APPENDIX **C**

CMTS MIBs Supported in Cisco IOS Release 12.1(20)EC and IOS Release 12.3(9a)BC

Table C-1 lists the MIBs that are included in Cisco IOS Release 12.1(20)EC and Cisco IOS Release 12.3(9a)BC for Cisco CMTS routers. Shaded cells indicate that the MIB is not included for that particular platform and software release. 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.

Table C-1 Included MIBs on Cisco CMTS Routers

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	**Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC**	**Cisco uBR10012 Cisco IOS Release 12.3(9a)BC**
ATM-MIB	ATM-MIB	ATM-MIB
BGP4-MIB	BGP4-MIB	BGP4-MIB
BRIDGE-MIB (-is- software images for 7100 only)	BRIDGE-MIB	
CISCO-AAL5-MIB	CISCO-AAL5-MIB	CISCO-AAL5-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-ACCESS-ENVMON-MIB	CISCO-ACCESS-ENVMON-MIB
CISCO-ATM-EXT-MIB	CISCO-ATM-EXT-MIB	CISCO-ATM-EXT-MIB
	CISCO-ATM-PVCTRAP-EXTN-MIB	CISCO-ATM-PVCTRAP-EXTN-MIB
	CISCO-BGP4-MIB	CISCO-BGP4-MIB
CISCO-BGP-POLICY-ACCOUNTIN G-MIB		
CISCO-BULK-FILE-MIB (-is- software images only)	CISCO-BULK-FILE-MIB (-is- software images only)	
CISCO-BUS-MIB (-is- software images only)	CISCO-BUS-MIB (-is- software images only)	
N	Not supported in Cisco 7100 series platform.	CISCO-CABLE-AVAILABILITY-MIB
	CISCO-CABLE-METERING-MIB	CISCO-CABLE-METERING-MIB
	CISCO-CABLE-QOS-MONITOR-MIB	CISCO-CABLE-QOS-MONITOR-MIB

Table C-1 Included MIBs on Cisco CMTS Routers (continued)

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC	Cisco uBR10012 Cisco IOS Release 12.3(9a)BC
CISCO-CABLE-SPECTRUM-MIB	CISCO-CABLE-SPECTRUM-MIB	CISCO-CABLE-SPECTRUM-MIB
CISCO-CALL-HISTORY-MIB	CISCO-CALL-HISTORY-MIB	
CISCO-CAR-MIB	CISCO-CAR-MIB	CISCO-CAR-MIB
CISCO-CASA-FA-MIB (-is- software images only)	CISCO-CASA-FA-MIB (-is- software images only)	
CISCO-CASA-MIB (-is- software images only)	CISCO-CASA-MIB (-is- software images only)	
CISCO-CDP-MIB	CISCO-CDP-MIB	CISCO-CDP-MIB
	CISCO-CIRCUIT-INTERFACE-MIB	CISCO-CIRCUIT-INTERFACE-MIB
CISCO-CLASS-BASED-QOS-MIB	CISCO-CLASS-BASED-QOS-MIB	
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB	CISCO-COMPRESSION-SERVICE-ADAPTER-MIB	
CISCO-CONFIG-COPY-MIB	CISCO-CONFIG-COPY-MIB	CISCO-CONFIG-COPY-MIB
CISCO-CONFIG-MAN-MIB	CISCO-CONFIG-MAN-MIB	CISCO-CONFIG-MAN-MIB
CISCO-DOCS-EXT-MIB	CISCO-DOCS-EXT-MIB	CISCO-DOCS-EXT-MIB
CISCO-DOCS-REMOTE-QUERY-MIB	CISCO-DOCS-REMOTE-QUERY-MIB	
CISCO-ENHANCED-MEMPOOL-MIB	CISCO-ENHANCED-MEMPOOL-MIB Supported only in Release 12.3(9a)BC and later releases.	CISCO-ENHANCED-MEMPOOL-MIB Supported only in Release 12.3(9a)BC and later releases.
	CISCO-ENTITY-ASSET-MIB	CISCO-ENTITY-ASSET-MIB
CISCO-ENTITY-EXT-MIB		
CISCO-ENTITY-FRU-CONTROL-MIB		
CISCO-ENTITY-SENSOR-MIB		
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-ENTITY-VENDORTYPE-OID-MIB
CISCO-ENVMON-MIB	CISCO-ENVMON-MIB	CISCO-ENVMON-MIB
CISCO-FLASH-MIB	CISCO-FLASH-MIB	CISCO-FLASH-MIB
CISCO-FRAME-RELAY-MIB	CISCO-FRAME-RELAY-MIB	CISCO-FRAME-RELAY-MIB
CISCO-FTP-CLIENT-MIB (-is- software images only)	CISCO-FTP-CLIENT-MIB (-is- software images only)	CISCO-FTP-CLIENT-MIB
CISCO-HSRP-EXT-MIB	CISCO-HSRP-EXT-MIB	CISCO-HSRP-EXT-MIB
CISCO-HSRP-MIB	CISCO-HSRP-MIB	CISCO-HSRP-MIB
CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-IETF-ATM2-PVCTRAP-MIB	CISCO-IETF-ATM2-PVCTRAP-MIB

Table C-1 Included MIBs on Cisco CMTS Routers (continued)

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC	Cisco uBR10012 Cisco IOS Release 12.3(9a)BC
	CISCO-IETF-IP-FORWARD-MIB	
	CISCO-IETF-IP-MIB	
	CISCO-IETF-NAT-MIB (-is- software images only)	
CISCO-IMAGE-MIB	CISCO-IMAGE-MIB	CISCO-IMAGE-MIB
CISCO-IP-ENCRYPTION-MIB		
CISCO-IPMROUTE-MIB	CISCO-IPMROUTE-MIB	CISCO-IPMROUTE-MIB
CISCO-IPSEC-FLOW-MONITOR-MIB	CISCO-IPSEC-FLOW-MONITOR-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-FLOW-MONITOR-MIB
CISCO-IPSEC-MIB	CISCO-IPSEC-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-MIB
CISCO-IPSEC-POLICY-MAP-MIB	CISCO-IPSEC-POLICY-MAP-MIB (-k8- or -k9- software images only)	CISCO-IPSEC-POLICY-MAP-MIB
CISCO-IP-STAT-MIB	CISCO-IP-STAT-MIB	CISCO-IP-STAT-MIB
CISCO-ISDN-MIB	CISCO-ISDN-MIB	
CISCO-LEC-DATA-VCC-MIB (-is- software images only)	CISCO-LEC-DATA-VCC-MIB (-is- software images only)	
CISCO-LEC-EXT-MIB (-is- software images only)	CISCO-LEC-EXT-MIB (-is- software images only)	
CISCO-LECS-MIB (-is- software images only)	CISCO-LECS-MIB (-is- software images only)	
CISCO-LES-MIB (-is- software images only)	CISCO-LES-MIB (-is- software images only)	
CISCO-MEMORY-POOL-MIB	CISCO-MEMORY-POOL-MIB	CISCO-MEMORY-POOL-MIB
	CISCO-NBAR-PROTOCOL-DISCOVERY-MIB	
CISCO-NDE-MIB		
	CISCO-NTP-MIB	CISCO-NTP-MIB
	CISCO-PIM-MIB	CISCO-PIM-MIB
CISCO-PING-MIB	CISCO-PING-MIB	CISCO-PING-MIB
	CISCO-PPPOE-MIB	
CISCO-PROCESS-MIB	CISCO-PROCESS-MIB	CISCO-PROCESS-MIB
CISCO-PRODUCTS-MIB	CISCO-PRODUCTS-MIB	CISCO-PRODUCTS-MIB
CISCO-QUEUE-MIB	CISCO-QUEUE-MIB	CISCO-QUEUE-MIB
CISCO-RMON-SAMPLING-MIB	CISCO-RMON-SAMPLING-MIB	CISCO-RMON-SAMPLING-MIB
CISCO-RTTMON-MIB	CISCO-RTTMON-MIB	CISCO-RTTMON-MIB

Table C-1 Included MIBs on Cisco CMTS Routers (continued)

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC	Cisco uBR10012 Cisco IOS Release 12.3(9a)BC
CISCO-SLB-EXT-MIB (-is- software images only)		
CISCO-SLB-MIB (-is- software images only)		
CISCO-SNAPSHOT-MIB	CISCO-SNAPSHOT-MIB	CISCO-SNAPSHOT-MIB
		CISCO-SRP-MIB
CISCO-SYSLOG-MIB	CISCO-SYSLOG-MIB	CISCO-SYSLOG-MIB
CISCO-TCP-MIB	CISCO-TCP-MIB	CISCO-TCP-MIB
	CISCO-VLAN-IFTABLE-RELATION SHIP-MIB	CISCO-VLAN-IFTABLE-RELATIONS HIP-MIB
CISCO-VPDN-MGMT-MIB (-is- software images only)	CISCO-VPDN-MGMT-MIB (-is- software images only)	
	CISCO-VPDN-MGMT-EXT-MIB (-is- software images only)	
	CISCO-VSIMASTER-MIB	
DOCS-BPI-MIB (-k8- or -k9- software images only)	DOCS-BPI-MIB (-k8- or -k9- software images only)	DOCS-BPI-MIB
	DOCS-BPI-PLUS-MIB (-k8- or -k9- software images only)	DOCS-BPI-PLUS-MIB
	DOCS-CABLE-DEVICE-MIB	DOCS-CABLE-DEVICE-MIB
	DOCS-CABLE-DEVICE-TRAP-MIB	DOCS-CABLE-DEVICE-TRAP-MIB
DOCS-IF-MIB	DOCS-IF-MIB	DOCS-IF-MIB
	DOCS-IF-EXT-MIB	DOCS-IF-EXT-MIB
	DOCS-QOS-MIB	DOCS-QOS-MIB
	DOCS-SUBMGT-MIB	DOCS-SUBMGT-MIB
	DSG-IF-MIB	DSG-IF-MIB
ENTITY-MIB	ENTITY-MIB	ENTITY-MIB
ETHERLIKE-MIB	ETHERLIKE-MIB	ETHERLIKE-MIB
	EVENT-MIB (-is- software images only)	EVENT-MIB
EXPRESSION-MIB (-is- software images only)	EXPRESSION-MIB (-is- software images only)	EXPRESSION-MIB
HC-RMON-MIB	HC-RMON-MIB	HC-RMON-MIB
IF-MIB	IF-MIB	IF-MIB
IGMP-MIB		
	IGMP-STD-MIB	IGMP-STD-MIB
INT-SERV-MIB	INT-SERV-MIB	INT-SERV-MIB

Table C-1 Included MIBs on Cisco CMTS Routers (continued)

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC	Cisco uBR10012 Cisco IOS Release 12.3(9a)BC
	IP-MIB	IP-MIB
IPMROUTE-MIB		
	IPMROUTE-STD-MIB	IPMROUTE-STD-MIB
ISDN-MIB	ISDN-MIB	
LAN-EMULATION-CLIENT-MIB (-is- software images only)	LAN-EMULATION-CLIENT-MIB (-is- software images only)	
	MSDP-MIB	MSDP-MIB
NOTIFICATION-LOG-MIB (not supported in -is- software images)	NOTIFICATION-LOG-MIB (not supported in -is- software images)	
OLD-CISCO-CHASSIS-MIB	OLD-CISCO-CHASSIS-MIB	OLD-CISCO-CHASSIS-MIB
OLD-CISCO-CPU-MIB	OLD-CISCO-CPU-MIB	OLD-CISCO-CPU-MIB
OLD-CISCO-INTERFACES-MIB	OLD-CISCO-INTERFACES-MIB	OLD-CISCO-INTERFACES-MIB
OLD-CISCO-IP-MIB	OLD-CISCO-IP-MIB	OLD-CISCO-IP-MIB
OLD-CISCO-MEMORY-MIB	OLD-CISCO-MEMORY-MIB	OLD-CISCO-MEMORY-MIB
OLD-CISCO-SYSTEM-MIB	OLD-CISCO-SYSTEM-MIB	OLD-CISCO-SYSTEM-MIB
OLD-CISCO-TCP-MIB	OLD-CISCO-TCP-MIB	OLD-CISCO-TCP-MIB
OLD-CISCO-TS-MIB	OLD-CISCO-TS-MIB	OLD-CISCO-TS-MIB
PIM-MIB	PIM-MIB	PIM-MIB
RFC1213-MIB	RFC1213-MIB	RFC1213-MIB
RFC1231-MIB	RFC1231-MIB	
RFC1253-MIB	RFC1253-MIB	RFC1253-MIB
RFC1315-MIB	RFC1315-MIB	RFC1315-MIB
RFC1381-MIB	RFC1381-MIB	
RFC1382-MIB	RFC1382-MIB	
RFC1406-MIB	RFC1406-MIB	RFC1406-MIB
RFC1407-MIB	RFC1407-MIB	RFC1407-MIB
	RFC1595-MIB	RFC1595-MIB
RFC2558-MIB		
RMON-MIB	RMON-MIB	RMON-MIB
RMON2-MIB	RMON2-MIB	RMON2-MIB
RS-232-MIB	RS-232-MIB	RS-232-MIB
RSVP-MIB	RSVP-MIB	RSVP-MIB
SMON-MIB	SMON-MIB	SMON-MIB
SNMP-COMMUNITY-MIB	SNMP-COMMUNITY-MIB	SNMP-COMMUNITY-MIB
SNMP-FRAMEWORK-MIB	SNMP-FRAMEWORK-MIB	SNMP-FRAMEWORK-MIB

Table C-1 Included MIBs on Cisco CMTS Routers (continued)

Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.1(20)EC	Cisco uBR7100 series and Cisco uBR7200 series Cisco IOS Release 12.3(9a)BC	Cisco uBR10012 Cisco IOS Release 12.3(9a)BC
SNMP-MPD-MIB	SNMP-MPD-MIB	SNMP-MPD-MIB
SNMP-NOTIFICATION-MIB	SNMP-NOTIFICATION-MIB	SNMP-NOTIFICATION-MIB
SNMP-PROXY-MIB	SNMP-PROXY-MIB	SNMP-PROXY-MIB
SNMP-TARGET-MIB	SNMP-TARGET-MIB	SNMP-TARGET-MIB
SNMP-USM-MIB	SNMP-USM-MIB	SNMP-USM-MIB
SNMPv2-MIB	SNMPv2-MIB	SNMPv2-MIB
SNMP-VACM-MIB	SNMP-VACM-MIB	SNMP-VACM-MIB
TCP-MIB	TCP-MIB	TCP-MIB
UDP-MIB	UDP-MIB	UDP-MIB

GLOSSARY

B

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

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

C

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

CM Cable Modem

CMTS Cable Modem Termination System

CNEM Consistent Network Element Manageability

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

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

CPE Customer Premises Equipment

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

CWDM Coarse Wavelength Division Multiplexing

D

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

DCD Downstream Channel Descriptor

DHCP Dynamic Host Configuration Protocol.

DMIC CMTS Dynamic Message Integrity Check

DOCSIS Data Over Cable System Interface specification

DOM Digital Optical Monitoring

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

DOCSIS Data-Over-Cable Service Interface Specification

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.

DSG DOCSIS Set-top Gateway

DWDM Dense Wavelength Division Multiplexing

E

EHSA Enhanced High System Availability.

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

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

F

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

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

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

G

Gb gigabit

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

Gbps gigabits per second

GB gigabyte

10GE 10 Gigabit per second Ethernet

H

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

I

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

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

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

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

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

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

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

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

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

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

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

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

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

J

No terms

K

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

L

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

LC Line Card

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.

LX/LH Long wavelength/long haul

M

MAC Media Access Control

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).

MSO Multisystem operator

MTU Maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

N

NAS Network access server. Cisco platform or collection of platforms such as an AccessPath system which interfaces between the Internet and the circuit world (the PSTN).

NMS Network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

NHLFE Next Hop Label Forwarding Entry.

O

OID Object identifier. Values are defined in specific MIB modules. The Event MIB allows you or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, you or an NMS configures a trigger entry in the mteTriggerTable of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and Boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

OIR Online Insertion and Removal.

OSM Optical Services Module

P

PAP Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but identifies the remote end. The router or access server determines if that user is allowed access. PAP is supported only on PPP lines.

PEM Power Entry Module.

Polling Access method in which a primary network device inquires, in an orderly fashion, whether secondaries have data to transmit. The inquiry occurs in the form of a message to each secondary that gives the secondary the right to transmit.

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.

QAM Quadrature Amplitude Modulation. Method of modulating digital signals onto a radio frequency carrier signal involving both amplitude and phase coding. QAM is a modulation scheme used in the downstream direction.

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

RF Channels Radio frequency channels

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.

RP Routing Processor

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

SAMIS Subscriber Account Management Interface Specification

Scalar object One type of managed object which is a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).

Security model A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SEEPROM Serial Electrically Erasable Programmable Read Only Memory.

SFP Small form-factor pluggable Gigabit Ethernet interfaces.

SID Service Identifier of cable modem.

SIP SPA interface processor. A SIP is a platform-specific carrier card that inserts into a router slot like a line card. A SIP can hold one or more SPAs in its subslots, depending on the SIP type. The SPA provides the network interface. The SIP provides the connection between the route processor (RP) and the SPA.

SFP Small Form-factor Pluggable (SFP) Gigabit Ethernet interfaces

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 within transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMP agent A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent.

SNMP manager A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

SONET Synchronous Optical Network. A physical layer interface standard for fiber optic transmission. High-speed synchronous network specification developed by Telcordia Technologies, Inc. and designed to run on optical fiber. STS-1 is the basic building block of SONET. Approved as an international standard in 1988.

SPA Shared port adapter. A SPA is a modular, platform-independent port adapter that inserts into a subslot of a compatible SIP carrier card to provide network connectivity and increased interface port density. The SPA provides the interface between the network and the SIP.

SX Short wavelength

T

TCP Transmission Control Protocol

TE Traffic Engineered

Time stamp Provides the amount of time that has elapsed between the last network reinitialization and generation of the trap.

TLV Type Length Value. Dynamic format for storing data in any order. Used by Cisco's Generic ID PROM for storing asset information.

Traffic engineering tunnel A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

Trap A 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.

UCID Upstream Channel ID

UDI Cisco Unique Device Identifier

UDP User Datagram Protocol.

US Upstream

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.

VPA Versatile Port Adapter. Same as the SPA.

VRF VPN Routing and Forwarding Tables.

W

WCM Wideband Cable Modem

WDCD Wideband Downstream Channel Descriptor

Write-only This variable can be used to set a new value for the variable only. For example, the writeMem variable, whose access is write-only, writes the current (running) router configuration into nonvolatile memory where it can be stored and retained even if the router is reloaded. If the value is set to 0, the writeMem variable erases the configuration memory.

Write view A view name (not to exceed 64 characters) for each group; the view name defines the list of object identifiers (OIDs) that can be created or modified by users of the group.

X

XENPAK Fiber-optic transceiver module which conforms to the 10GbE

Z

ZX Extended reach GBIC

INDEX

A

AAL5 3-8, 3-9, 3-10
alarms
  enabling traps A-14
  monitoring A-15
asset tracking 3-31
asset tracking information A-6
ATM
  broadcast and unknown server (BUS) management 3-11
  circuit management 3-21
  LANE management 3-85
  LEC extensions 3-45
  LEC management 3-45
  LES management 3-46
  managing PVCs 3-10
  VCL extensions 3-41
  VLAN management 3-11
  VSI management 3-55
ATM adaption layer 5 3-8, 3-9, 3-10
ATM-MIB 3-7

B

baseline privacy interface (BPI) management 3-55
baseline privacy interface plus (BPI+) management 3-55
basic information A-3
BGP4-MIB 3-8
Border Gateway Protocol (BGP) 3-8, 3-10
  policy accounting 3-11
BRIDGE-MIB 3-8
bulk-file operations 3-11
burst intervals, displaying A-18

C

cable modem max-cpe command 3-66
cable modems
  displaying burst and station maintenance intervals A-18
  displaying current status A-17
  displaying flap list information A-32
cable sflog command 3-65, A-19
cable upstream connector command 3-77
CASA management 3-20
ccqmCmtsEnforceRuleTable A-34
ccqmEnfRuleViolateTable B-2
ccsSNRRequestTable A-24
ccsSpectrumDataTable A-23
ccsUpSpecMgmtTable A-26
CDP management 3-20
cdrqCmtsCmStatusTable B-10
cdxBWQueueTable B-4
cdxCmCpeTable B-5
cdxCmtsCmStatusExtTable B-6
cdxCmtsServiceExtTable B-4
cdxIfUpstreamChannelExtTable B-8
cdxQosCtrlUpTable B-3
changes in this guide 3-xv
chassis
  asset information A-6
  displaying chassis ID and serial number A-3
  displaying component model names A-4
  displaying component serial numbers A-4
  displaying hardware components A-4

displaying hardware revision A-4
enabling traps for physical hardware changes A-14
monitoring FRUs A-6
OIDs for all physical components A-6
performing inventory management A-6
chassisId A-3
chassis traps 4-17
Cisco 7600 series Internet router
enhanced management feature 1-2
CISCO-AAA-SERVER-MIB 3-8, 3-9
CISCO-AAL5-MIB 3-8, 3-9
CISCO-ACCESS-ENVMON-MIB 3-9
CISCO-ATM-EXT-MIB 3-10
CISCO-ATM-PVCTRAP-EXTN-MIB 3-10
CISCO-BGP4-MIB 3-10
CISCO-BGP-POLICY-ACCOUNTING-MIB 3-11
CISCO-BULK-FILE-MIB 3-11
CISCO-BUS-MIB 3-11
CISCO-CABLE-AVAILABILITY-MIB 3-12
CISCO-CABLE-METERING-MIB 3-13
CISCO-CABLE-QOS-MONITOR-MIB 3-13, A-34, B-2
using subscriber traffic management A-34
CISCO-CABLE-SPECTRUM-MIB 3-14, 3-15, A-20
configuring flap lists A-29
displaying flap lists A-29, A-30
monitoring spectrum management A-20
CISCO-CALL-HISTORY-MIB 3-15
CISCO-CAR-MIB 3-19
CISCO-CASA-FA-MIB 3-20
CISCO-CASA-MIB 3-20
CISCO-CDP-MIB 3-20
CISCO-CIRCUIT-INTERFACE-MIB 3-21
CISCO-CLASS-BASED-QOS-MIB 3-21
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB 3-25
CISCO-CONFIG-COPY-MIB 3-25
CISCO-CONFIG-MAN-MIB 3-26
CISCO-DOCS-EXT-MIB 3-26, A-18, B-3, B-4, B-5, B-6, B-8
burst and station maintenance intervals A-18
CISCO-DOCS-REMOTE-QUERY-MIB 3-29, B-10
CISCO-ENHANCED-MEMPOOL-MIB 3-30
CISCO-ENTITY-ALARM-MIB 3-31
CISCO-ENTITY-ASSET-MIB 3-31, A-6
CISCO-ENTITY-EXT-MIB 3-32
CISCO-ENTITY-FRU-CONTROL-MIB 3-32, A-6, A-14
CISCO-ENTITY-SENSOR-MIB 3-33
CISCO-ENTITY-VENDORTYPE-OID-MIB 3-34, A-6
CISCO-ENVMON-MIB 3-37, A-6, A-14
Cisco Express Forwarding (CEF) 2-6
CISCO-FLASH-MIB 3-39
CISCO-FRAME-RELAY-MIB 3-39
CISCO-FTP-CLIENT-MIB 3-40
CISCO-HSRP-EXT-MIB 3-40
CISCO-HSRP-MIB 3-40
CISCO-IETF-ATM2-PVCTRAP-MIB 3-41
CISCO-IETF-IP-FORWARD-MIB 3-41
CISCO-IETF-IP-MIB 3-41
CISCO-IETF-NAT-MIB 3-42
CISCO-IMAGE-MIB 3-42
Cisco IOS Release 12.3(23)BC
MIB support 3-2
Cisco IOS software image management 3-42
CISCO-IP-ENCRYPTION-MIB 3-43
CISCO-IPMROUTE-MIB 3-43
CISCO-IPSEC-FLOW-MONITOR-MIB 3-44
CISCO-IPSEC-MIB 3-44
CISCO-IPSEC-POLICY-MAP-MIB 3-44
CISCO-IP-STAT-MIB 3-43
CISCO-ISDN-MIB 3-44
CISCO-LEC-DATA-VCC-MIB 3-45
CISCO-LEC-EXT-MIB 3-45
CISCO-LECS-MIB 3-45
CISCO-LES-MIB 3-46
CISCO-MEMORY-POOL-MIB 3-46
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB 3-46
CISCO-NDE-MIB 3-47
CISCO-NTP-MIB 3-47
CISCO-PIM-MIB 3-48

CISCO-PING-MIB 3-48
CISCO-PPPOE-MIB 3-48
CISCO-PROCESS-MIB 3-48
CISCO-PRODUCTS-MIB 3-49
CISCO-QUEUE-MIB 3-50
CISCO-RMON-SAMPLING-MIB 3-50
CISCO-RTTMON-MIB 3-50
CISCO-SLB-EXT-MIB 3-51
CISCO-SLB-MIB 3-51
CISCO-SNAPSHOT-MIB 3-51
CISCO-SRP-MIB 3-52
CISCO-SYSLOG-MIB 3-52, A-14, A-15
    monitoring system messages A-15
CISCO-TCP-MIB 3-52
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB 3-53
CISCO-VPDN-MGMT-EXT-MIB 3-53
CISCO-VPDN-MGMT-MIB 3-54
CISCO-VSIMASTER-MIB 3-55
clogHistoryTable A-15
commands, SNMP 2-5
community strings management 3-93
compiling MIBs 2-4
configuration files
    copying 3-25
    tracking changes 3-26
counters
    32-bit and 64-bit values A-2
    clearing A-2
    difference between CLI and SNMP counters A-2
    interface counter cache A-1
CPU process management 3-48

D

displaying CNR measurements for a cable modem A-24
displaying frequency hops A-26
displaying information about burst and station maintenance intervals A-18
displaying information about cable modems A-17
DMIC 3-26, 3-28, 3-29
DOCS-BPI-MIB 3-55
DOCS-BPI-PLUS-MIB 3-55
DOCS-CABLE-DEVICE-MIB 3-56
DOCS-CABLE-DEVICE-TRAP-MIB 3-57
docsIfCmtsCmStatusTable B-11
docsIfCmtsModulationTable B-13
docsIfCmtsServiceTable B-19
DOCS-IF-EXT-MIB 3-58
DOCS-IF-MIB 3-58, B-10, B-11, B-13
    Cisco-specific extensions 3-26
    displaying information about cable modems A-17
docsIfSignalQualityTable B-10
DOCSIS
    BPI+ management 3-55
    BPI management 3-55
    device management 3-56
    interface extensions 3-58
    interface management 3-58
    QoS management 3-64
    remote query 3-29
    subscriber management 3-66
    trap management 3-57
DOCSIS 3.0
    Downstream Channel Bonding 2-7
DOCS-QOS-MIB 3-64, B-15, B-17, B-19, B-20, B-21, B-24
docsQosParamSetTable B-17
docsQosPHSTable B-24
docsQosPktTable B-15
docsQosServiceClassTable B-21
docsQosServiceFlowIdTable B-19
docsQosServiceFlowStatsTable B-20
docsQosUpstreamStatsTable B-20
DOCS-SUBMGT-MIB 3-66
docsSubMgtPktFilterTable B-24
docsSubMgtTcpUdpFilterTable B-25
DOCS-SUBSCRIBER-MIB B-24, B-25
document revision history 3-xv
downloading MIBs 2-3, 2-4

Downstream (DS) channel bandwidth utilization 3-12
DS1 management 3-91
DS3 management 3-91
DSG-IF-MIB 3-62
dynamic feedback protocol (DFP) 3-51
dynamic shared secret 3-26

E

E1 management 3-91
E3 management 3-91
EIA/TIA-232 management 3-93
enabling
  SNMP 2-4
entAliasMappingTable A-5
ENTITY-MIB 3-68, A-4, A-5
  asset tracking 3-31
  extensions 3-32
  FRU management 3-32
  inventory management A-6
  managing physical components A-5
  mapping to IF-MIB A-5
  OID definitions 3-34
  sensors extensions 3-33
entPhysicalContainsTable A-5
entPhysicalDescr A-4
entPhysicalHardwareRev A-4
entPhysicalIndex A-5
entPhysicalModelName A-4
entPhysicalSerialNum A-4
entPhysicalTable A-5
environmental monitoring 3-9, 3-37
environmental sensors, displaying A-6
environmental traps A-14
ENVON-MIB
  Cisco-specific extensions 3-37
ETHERLIKE-MIB 3-77
Ethernet management 3-77
EVENT-MIB 3-78
events management 3-78
EXPRESSION-MIB 3-78

F

FAQs, SNMP and Cisco MIBs 1-8
File Transfer Protocol (FTP)
  management 3-40
flap lists
  clearing counters A-33
  configuring A-29
  displaying A-30
  displaying information for a specific cable modem A-32
flap-list troubleshooting A-29
  troubleshooting suggestions A-30
  using SNMP A-29, A-30, A-33
flash card traps 4-7
Flash memory
  management 3-39
Frame-relay
  circuit management 3-21
  DTE management 3-90
  management 3-39
frequency hops
  displaying A-26
FRUs
  enabling traps A-14
  management 3-32
  monitoring A-6

G

generating traps A-12

H

hardware management 3-68
hardware OIDs 3-49

hardware revision, displaying A-4
HCCP management 3-12
HC-RMON-MIB 3-79
high CPU usage 2-5
hostname command A-3
HSRP management 3-40

I

ICMP
- management 3-41
- Ping management 3-48

IF-MIB 3-79
- counter cache A-1
- mapping to ENTITY-MIB A-5

ifTable
- counter cache A-1

IGMP-STD-MIB 3-83
integrated services protocol (ISP) 3-83
interface
- management 3-79
- queue management 3-50

INT-SERV-MIB 3-83
inventory management A-6
IOS software image management 3-42
IP
- encryption management 3-43
- IGMP management 3-83
- ISP management 3-83
- management 3-41, 3-84
- MSDP management 3-85
- multicasting routing 3-84
- multicast management 3-43
- multicast routing 3-84
- NAT management 3-42
- PIM management 3-48, 3-88
- statistics 3-43
- TCP management 3-52, 3-96
- UDP management 3-96

ip accounting mac-address command 3-43
ip accounting precedence command 3-43
IP forwarding 3-41
IP-MIB 3-84
IPMROUTE-MIB 3-84
IPMROUTE-STD-MIB 3-84
IPSec
- management 3-44
- policy management 3-44

ISDN management 3-44
ISDN-MIB 3-85

L

LANE 3-11
LAN-EMULATION-CLIENT-MIB 3-85
LAPB management 3-90
Layer 2 bridging 3-8
line cards
- traps 4-7

linkUp and linkDown traps 4-8, 4-9, 4-10, 4-16

M

managing physical components A-4
mapping IF-MIB and ENTITY-MIB A-5
memory management 3-46
Memory statistics 3-30
message processing and dispatching (MPD) 3-94
MIB descriptions
- ATM 3-7
- BGP4-MIB 3-8
- BRIDGE-MIB 3-8
- CISCO-AAA-SERVER-MIB 3-8, 3-9
- CISCO-AAL5-MIB 3-8, 3-9
- CISCO-ACCESS-ENVMON-MIB 3-9
- CISCO-ATM-EXT-MIB 3-10
- CISCO-ATM-PVCTRAP-EXTN-MIB 3-10

CISCO-BGP4-MIB 3-10
CISCO-BGP-POLICY-ACCOUNTING-MIB 3-11
CISCO-BULK-FILE-MIB 3-11
CISCO-BUS-MIB 3-11
CISCO-CABLE-AVAILABILITY-MIB 3-12
CISCO-CABLE-QOS-MONITOR-MIB 3-13
CISCO-CABLE-SPECTRUM-MIB 3-14, 3-15
CISCO-CALL-HISTORY-MIB 3-15
CISCO-CAR-MIB 3-19
CISCO-CASA-FA-MIB 3-20
CISCO-CASA-MIB 3-20
CISCO-CDP-MIB 3-20
CISCO-CIRCUIT-INTERFACE-MIB 3-21
CISCO-CLASS-BASED-QOS-MIB 3-21
CISCO-COMPRESSION-SERVICE-ADAPTER-MIB 3-25
CISCO-CONFIG-COPY-MIB 3-25
CISCO-CONFIG-MAN-MIB 3-26
CISCO-DOCS-EXT-MIB 3-26
CISCO-DOCS-REMOTE-QUERY-MIB 3-29
CISCO-ENHANCED-MEMPOOL-MIB 3-30
CISCO-ENTITY-ALARM-MIB 3-31
CISCO-ENTITY-ASSET-MIB 3-31
CISCO-ENTITY-EXT-MIB 3-32
CISCO-ENTITY-FRU-CONTROL-MIB 3-32
CISCO-ENTITY-SENSOR-MIB 3-33
CISCO-ENTITY-VENDORTYPE-OID-MIB 3-34
CISCO-ENVMON-MIB 3-37
CISCO-FLASH-MIB 3-39
CISCO-FRAME-RELAY-MIB 3-39
CISCO-FTP-CLIENT-MIB 3-40
CISCO-HSRP-EXT-MIB 3-40
CISCO-HSRP-MIB 3-40
CISCO-IETF-ATM2-PVCTRAP-MIB 3-41
CISCO-IETF-IP-FORWARD-MIB 3-41
CISCO-IETF-IP-MIB 3-41
CISCO-IETF-NAT-MIB 3-42
CISCO-IMAGE-MIB 3-42
CISCO-IP-ENCRYPTION-MIB 3-43
CISCO-IPMROUTE-MIB 3-43
CISCO-IPSEC-FLOW-MONITOR-MIB 3-44
CISCO-IPSEC-MIB 3-44
CISCO-IPSEC-POLICY-MAP-MIB 3-44
CISCO-IP-STAT-MIB 3-43
CISCO-ISDN-MIB 3-44
CISCO-LEC-DATA-VCC-MIB 3-45
CISCO-LEC-EXT-MIB 3-45
CISCO-LECS-MIB 3-45
CISCO-LES-MIB 3-46
CISCO-MEMORY-POOL-MIB 3-46
CISCO-NBAR-PROTOCOL-DISCOVERY-MIB 3-46
CISCO-NDE-MIB 3-47
CISCO-NTP-MIB 3-47
CISCO-PIM-MIB 3-48
CISCO-PING-MIB 3-48
CISCO-PPPOE-MIB 3-48
CISCO-PROCESS-MIB 3-48
CISCO-PRODUCTS-MIB 3-49
CISCO-QUEUE-MIB 3-50
CISCO-RMON-SAMPLING-MIB 3-50
CISCO-RTTMON-MIB 3-50
CISCO-SLB-EXT-MIB 3-51
CISCO-SLB-MIB 3-51
CISCO-SNAPSHOT-MIB 3-51
CISCO-SRP-MIB 3-52
CISCO-SYSLOG-MIB 3-52
CISCO-TCP-MIB 3-52
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB 3-53
CISCO-VPDN-MGMT-EXT-MIB 3-53
CISCO-VPDN-MGMT-MIB 3-54
CISCO-VSIMASTER-MIB 3-55
DOCS-BPI-MIB 3-55
DOCS-BPI-PLUS-MIB 3-55
DOCS-CABLE-DEVICE-MIB 3-56
DOCS-CABLE-DEVICE-TRAP-MIB 3-57
DOCS-IF-EXT-MIB 3-58

DOCS-IF-MIB 3-58
DOCS-QOS-MIB 3-64
DOCS-SUBMGT-MIB 3-66
ENTITY-MIB 3-68
ETHERLIKE-MIB 3-77
EVENT-MIB 3-78
EXPRESSION-MIB 3-78
HC-RMON-MIB 3-79
IF-MIB 3-79
IGMP-STD-MIB 3-83
INT-SERV-MIB 3-83
IP-MIB 3-84
IPMROUTE-MIB 3-84
IPMROUTE-STD-MIB 3-84
ISDN-MIB 3-85
LAN-EMULATION-CLIENT-MIB 3-85
MSDP-MIB 3-85
NOTIFICATION-LOG-MIB 3-86
OLD-CISCO-CHASSIS-MIB 3-87
OLD-CISCO-CPU-MIB 3-87
OLD-CISCO-INTERFACES-MIB 3-87
OLD-CISCO-IP-MIB 3-88
OLD-CISCO-MEMORY-MIB 3-88
OLD-CISCO-SYSTEM-MIB 3-88
OLD-CISCO-TCP-MIB 3-88
OLD-CISCO-TS-MIB 3-88
PIM-MIB 3-88
RFC1213-MIB 3-89
RFC1231-MIB 3-89
RFC1253-MIB 3-89
RFC1315-MIB 3-90
RFC1381-MIB 3-90
RFC1382-MIB 3-90
RFC1406-MIB 3-91
RFC1407-MIB 3-91
RFC1595-MIB 3-91
RFC2558-MIB 3-92
RMON2-MIB 3-92
RMON-MIB 3-92
RS-232-MIB 3-93
RSVP-MIB 3-93
SMON-MIB 3-93
SNMP-COMMUNITY-MIB 3-93
SNMP-FRAMEWORK-MIB 3-94
SNMP-MPD-MIB 3-94
SNMP-NOTIFICATION-MIB 3-94
SNMP-PROXY-MIB 3-95
SNMP-TARGET-MIB 3-95
SNMP-USM-MIB 3-95
SNMPv2-MIB 3-96
SNMP-VACM-MIB 3-96
TCP-MIB 3-96
UDP-MIB 3-96
MIBs
benefits 1-2
compiling 2-4
downloading 2-3, 2-4
OID assignments 1-3
overview 1-1, 1-2, 1-3
RFCs 1-7
useful information 2-3
MIB specifications, see MIB descriptions
model names, displaying A-4
model number, displaying A-3
module traps 4-17
monitoring
alarms A-15
monitoring alarms A-15
monitoring spectrum management A-20
MSDP-MIB 3-85
multicast routing
management 3-43, 3-84
PIM management 3-88
multicast source discovery protocol (MSDP) 3-85

N

N+1 redundancy 3-12

NBAR management 3-46
NDE management 3-47
Netflow
management 3-47
Network Address Translation (NAT)
management 3-42
Network-Based Application Recognition (NBAR) 3-46
Network Time Protocol (NTP)
management 3-47
new in this guide 3-xv
NOTIFICATION-LOG-MIB 3-86
notifications
defined 4-1
management 3-94
nruCacheSnmpData 3-86

O

object identifiers (OIDs) 1-3
Obtaining Documentation and Submitting a Service Request 3-xx
OLD-CISCO-CHASSIS-MIB 3-87, A-3
OLD-CISCO-CPU-MIB 3-87
OLD-CISCO-INTERFACES-MIB 3-87
OLD-CISCO-IP-MIB 3-88
OLD-CISCO-MEMORY-MIB 3-88
OLD-CISCO-SYSTEM-MIB 3-88
OLD-CISCO-TCP-MIB 3-88
OLD-CISCO-TS-MIB 3-88
open shortest path first (OSPF) routing management 3-89
OSPF 3-89
outages, monitoring A-15

P

physical components, managing A-4
physical hardware management 3-68
PIM management 3-48
PIM-MIB 3-88
Ping management 3-48
Point-to-Point Protocol over Ethernet (PPPoE) 3-48
power supply, failures 3-9
PPPoE management 3-48
process management 3-48
product OIDs 3-49
progression process for RF 4-20
protocol independent multicast (PIM)
management 3-88
PVCs, managing 3-10

Q

QoS
configuration management 3-21
DOCSIS management 3-64
subscriber traffic management 3-13
queue management 3-50

R

redundancy framework traps 4-20
remote query 3-29
resource reservation protocol (RSVP) 3-93
RFC 1213 3-84, 3-89
RFC1213-MIB 3-89
RFC 1231 3-89
RFC1231-MIB 3-89
RFC 1253 3-89
RFC1253-MIB 3-89
RFC 1315 3-39, 3-90
RFC1315-MIB 3-90
RFC 1381 3-90
RFC1381-MIB 3-90
RFC 1382 3-90
RFC1382-MIB 3-90
RFC 1406 3-91
RFC1406-MIB 3-91

RFC 1407 3-91
RFC1407-MIB 3-91
RFC 1493 3-8
RFC 1595 3-91
RFC1595-MIB 3-91
RFC 1657 3-8
RFC 1659 3-93
RFC 1757 3-92
RFC 1907 3-96
RFC 2011 3-41, 3-84
RFC 2012 3-96
RFC 2013 3-96
RFC 2096 3-41
RFC 2127 3-85
RFC 2206 3-93
RFC 2233 3-79
RFC 2558 3-92
RFC2558-MIB 3-92
RFC 2571 3-94
RFC 2572 3-94
RFC 2573 3-94, 3-95
RFC 2574 3-95
RFC 2575 3-96
RFC 2576 3-93
RFC 2613 3-93
RFC 2665 3-77, 3-79
RFC 2669 3-56
RFC 2670 3-58, 3-79
RFC 2737 3-68
RFC 2737, see ENTITY-MIB
RFC 2932 3-84
RFC 2933 3-83
RFC 2934 3-88
RFC 3014 3-86
RFC 3022 3-42
RFC 3083 3-55
RFCs, description 1-7
RF notifications 4-21
RF spectrum management 3-14, 3-15
RMON
  management 3-79, 3-92
  RMON-2 management extensions 3-92
  round-trip time (RTT) management 3-50
  sampling 3-50
  SMON management 3-93
RMON2-MIB 3-92
RMON-MIB 3-92
RS-232-MIB 3-93
RSVP-MIB 3-93
RTT management 3-50
running time, displaying A-3

S

security levels, SNMP 1-6
sensor management 3-33
serial number, displaying A-3, A-4
server load balancing (SLB) 3-51
service-level agreement
  enforcement 3-13
show cable device access-group command B-5, B-6
show cable filter command B-24, B-25
show cable flap-list command A-32
show cable modem classifiers command B-15
show cable modem command B-6, B-11
show cable modem connectivity command B-6, B-8
show cable modem remote-query command B-10
show cable modulation-profile command B-13
show cable qos enforce-rule command B-2
show cable service-class command B-17, B-21
show cable subscriber-usage command B-2
show controllers cable upstream spectrum command A-23
show interface cable modem command B-6
show interface cable qos paramset command B-17, B-21, B-22
show interface cable service-flow command B-19, B-24
show interface cable sid command B-20
show interface cable sid counter command B-4

show interface cable signal-quality command B-10
show interface cable upstream and show interface cable mac-scheduler command B-4, B-5
show interface cable upstream command B-3, B-5, B-8, B-11
show interface cable upstream ugs statistics command B-9
show interface command 3-79, B-1
show subsys command 2-2
SIP GL-8
SMON-MIB 3-93
snapshot routing 3-51
SNMP
  benefits 1-2
  ccsSNRRequestTable A-24
  ccsSpectrumDataTable A-23
  ccsUpSpecMgmtTable A-26
  configuration information 1-8
  controlling high CPU usage 2-5
  displaying flap lists A-29
  displaying frequency hops A-26
  displaying information about burst and station maintenance intervals A-18
  displaying information about cable modems A-17
  enabling 2-4
  FAQs 1-8
  generating traps A-12
  inventory management A-6
  managing physical components A-4
  MIBs 1-1, 1-2, 1-3
  monitoring CNR measurements A-24
  monitoring spectrum management A-20
  obtaining basic information about the router A-3
  OIDs 1-3
  related information 1-7
  security 1-6
  synchornizing between redundant PRE modules A-2
  using subscriber traffic management A-34
  versions 1-5
SNMP agent 4-2
SNMP commands 2-5
SNMP-COMMUNITY-MIB 3-93
SNMP-FRAMEWORK-MIB 3-94
SNMP-MPD-MIB 3-94
SNMP-NOTIFICATION-MIB 3-94
  generating traps A-13
SNMP-PROXY-MIB 3-95
snmp-server chassis-id command 3-87, A-3
snmp-server community command 2-4
snmp-server contact command A-4
snmp-server enable traps alarms command A-14
snmp-server enable traps entity command A-14
snmp-server enable traps envmon command A-14
snmp-server enable traps fru-ctrl command A-14
snmp-server enable traps syslog command A-14, A-16
snmp-server location command A-4
snmp-server queue-length command 3-52
snmp-server view command 2-4, 2-6
SNMP-TARGET-MIB 3-95
  generating traps A-12
SNMP traps 1-5
  chassis and module 4-17
  description 1-5
  environmental conditions 4-19
  flash card 4-7
  line card 4-7
  linkUp and linkDown 4-8, 4-9, 4-10, 4-16
SNMP-USM-MIB 3-95
SNMPv1 1-5
SNMPv2c 1-5
SNMPv2-MIB 3-96
SNMPv3 1-5, GL-9
SNMP-VACM-MIB 3-96
SONET/SDH
  management 3-92
SONET/SDH management 3-91
SPA Interface Processor. Line GL-8
spatial reuse protocol (SRP) 3-52
specifications 1-8
specifications, MIB

see MIB descriptions
spectrum management 3-14, 3-15
displaying frequency hops A-26
displaying the results of a spectrum request A-23
enabling A-21
monitoring A-20
monitoring CNR measurements A-24
standards 1-8
station maintenance intervals, displaying A-18
subscriber management 3-66, A-34
configuring A-34
displaying violators A-35
enabling traps A-36
subscriber traffic management 3-13
Switch of Activity for RF 4-20
synchronizing SNMP commands between redundant PRE modules A-2
sysContact A-4
sysDescr, displaying A-3
sysLocation A-4
SYSLOG
enabling traps A-14, A-16
management A-15
monitoring messages A-15
syslog management 3-52
sysName A-3
sysObjectID A-3
system contact information, displaying A-4
system description, displaying A-3
system location, displaying A-4
system log management 3-52
system message logs A-15
system name, displaying A-3
sysUpTime A-3

T

T1 management 3-91
T3 management 3-91
TCP management 3-52, 3-96
TCP-MIB 3-96
traps
common notifications A-13
enabling alarm traps A-14
enabling environmental traps A-14
enabling for FRU changes A-14
enabling for subscriber management A-36
enabling SYSLOG messages A-16
enabling SYSLOG traps A-14
enabling traps for physical hardware changes A-14
generating A-12, A-13
troubleshooting high CPU usage 2-5

U

UDP management 3-96
UDP-MIB 3-96
up time, displaying A-3
user-based security model (USM)
management 3-95

V

view-based access control model (VACM)
management 3-96
VLAN
extensions 3-53
management 3-53
VPDN
management 3-54

X

X.25
management 3-90