Cisco NCS 4000 Series MIB Specifications Guide

Cisco IOS XR Software

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

Cisco NCS 4000 Series Routers MIB Specifications Guide

Contents

Contents

Contents

Contents

Contents

Contents

Preface

This guide describes the implementation of the Simple Network Management Protocol (SNMP) and Management Information Base (MIB) for Cisco NCS 4000 Series Aggregation Services Routers. SNMP provides a set of commands for setting and retrieving the values of operating parameters on the Cisco NCS 4000 Series router. The router information is stored in a virtual storage area called a Management Information Base (MIB), which contains many MIB objects that describe router components and provides information about the status of the components.
This preface provides an overview of this guide with the following sections:

Audience

This guide is intended for system and network administrators who must configure the Cisco NCS 4000 Series router for operation and monitor its performance in the network.

This guide may also be useful for application developers who are developing management applications for the Cisco NCS 4000 Series router.

Organization

This guide contains the following chapters:

Chapter	Description
Chapter 1, “Chapter 1 - Cisco NCS 4000 Series Routers MIB Overview”	Provides background information about SNMP and its implementation on the Cisco NCS 4000 Series router.
Chapter 2, “Chapter 2 - Configuring MIB Support”	Provides instructions for configuring SNMP management support on the Cisco NCS 4000 Series router.
Chapter 3, “Cisco NCS 4000 Series Routers MIB Specifications”	Describes each MIB included on the Cisco NCS 4000 Series router. Each description lists any constraints as to how the MIB is implemented on the router.
Chapter 4, “Monitoring Notifications”	Describes the SNMP notifications supported by the Cisco NCS 4000 Series router, provides a description of each notification, a probable cause, and recommended action to take.

Terminology and Definitions

This section discusses conventions and terminology used in this guide.

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

Note: Many commands use the word traps in the command syntax. Unless there is an option in the command to select traps. Use the snmp-server host and snmp-server notification command to specify whether to send SNMP notifications as traps.

- Element Management System (EMS)—An EMS manages a specific portion of the network. For example, the SunNet Manager, an SNMP management application, is used to manage SNMP-manageable elements. Element Managers may manage asynchronous lines, multiplexers, Private Automatic Branch Extension (PABX), proprietary systems, or an application.
- Management Information Base (MIB)—The management objects available in an SNMP managed device. The information is represented in Abstract Syntax Notation 1 (ASN.1). This is a way of logically grouping data so that it is easily understood by all.
- MIB-II—The successor to MIB-I, which was the original standard SNMP MIB.
- Multiprotocol Label Switching (MPLS)—MPLS is the standardized version of the Cisco original tag-switching proposal. It uses a label-forwarding paradigm (forward packets based on labels).
- Simple Network Management Protocol (SNMP)—An application layer protocol that allows you to remotely manage networked devices. The simple in SNMP is only in contrast to protocols that are thought to be even more complex than SNMP. SNMP consists of the following components: a management protocol, a definition of management information and events, a core set of management information and events, and a mechanism and approach used to manage the use of the protocol including security and access control.
- Trap—A device-initiated SNMP notification message. The contents of the message might be simply informational, but it is mostly used to report real-time trap information. Traps can be used in conjunction with other SNMP mechanisms, as in trap-directed polling.
- User Datagram Protocol (UDP)—A connectionless, non-reliable IP-based transport protocol.

Obtaining Documentation and Submitting a Service Request

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

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

Subscribe to the *What's New in Cisco Product Documentation* as 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 NCS 4000 Series Routers MIB Overview

This chapter provides an overview of the Cisco NCS 4000 Series router management feature. This chapter contains the following topics:

Benefits of MIB Enhancements

The Cisco NCS 4000 Series router management feature allows the router to be managed through the Simple Network Management Protocol (SNMP).

Using the Cisco NCS 4000 Series router management feature, you can:

- Manage and monitor the Cisco NCS 4000 Series router resources through an SNMP-based Network Management System (NMS)
- Use SNMP **set** and **get** requests to access information in Cisco NCS 4000 Series Series router MIBs
- Reduce the amount of time and system resources required to perform functions such as inventory management

Other benefits include:

- A standards-based technology (SNMP) for monitoring faults and performance on the router
- Support for all SNMP versions (SNMPv1, SNMPv2c, and SNMPv3)
- Notification of faults, alarms, and conditions that might affect services
- A way to access router information other than through the Command-Line Interface (CLI) or Extensible Markup Language (XML).

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has three parts:

- SNMP manager—A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a NMS. The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).
- SNMP agent—A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent (see the "Enabling SNMP Support" section on page 17).

- Management Information Base (MIB)— A MIB is a database of objects that can be managed on a device. This database describes various components and provides information about the attributes of the components of a network device.

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

MIB Description

A MIB is a database of the objects that can be managed on a device. The managed objects or variables can be set or read to provide information on the network devices and interfaces and are organized hierarchically. The MIB consists of collections of managed objects identified by object identifiers. MIBs are accessed using a network management protocol such as SNMP. A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device, such as a router. Managed objects comprise one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs contain two types of managed objects:

- Scalar objects—Define a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).
- Columnar objects—Define multiple related objects such as zero, one, or more instances at any point in time that are grouped together in MIB tables (for example, ifTable in the IF-MIB defines the interface).

System MIB variables are accessible through SNMP as follows:

- Accessing a MIB variable—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- Setting a MIB variable—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP Notifications

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

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

When an agent detects an alarm condition, the agent:

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

SNMP notifications are sent as one of the following:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.

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. A SNMP notification is sent as *traps*. See the "Enabling Notifications" for instructions on how to enable notifications and traps on the Cisco NCS 4000 Series router. Use the **snmp-server host** command to specify that SNMP notifications are sent as traps. See Chapter 4, "Monitoring Notifications," for information about Cisco NCS 4000 Series router traps.

SNMP Versions

Cisco IOS XR Software supports the following versions of SNMP:

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

SNMPv1 and SNMPv2c

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

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

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

SNMPv3

SNMPv3 provides security models and security levels:

- A security *model* is an authentication strategy that is set up for a user and the group in which the user resides.
- A security *level* is the permitted level of security within a security model.
- A combination of a security model and a security level determines the security mechanism employed when handling an SNMP packet.

SNMP Security Models and Levels

The following table describes the security models and levels provided by the different SNMP versions.

Table 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 XR Software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Requests for Comments

MIB modules are typically defined in Request for Comment (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 getting RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (http://www.isoc.org and http://www.ietf.org).

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

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA).
- Enterprise MIB OIDs are assigned by Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.xyz represents the.*xyz* with the location in the MIB hierarchy as follows. Note that the numbers in parentheses are included to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

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

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1).

For a list of OIDs assigned to MIB objects, go to the following URL:

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

SNMP Configuration Information

The following references provide information about configuring SNMP:

- *Implementing SNMP* module provides general information about configuring and implementing SNMP support. It is part of the *Cisco IOS XR System Management Configuration Guide.*
- *SNMP Server Commands* module provides information about SNMP commands. It is part of the
- Cisco IOS XR System Management Command Reference.

Chapter 2 - Configuring MIB Support

This chapter describes how to configure SNMP and MIB support for the Cisco NCS 4000 Series router. It includes the following sections:

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the Cisco NCS 4000 Series router:

Considerations for Working with MIBs

While working with MIBs, consider the following:

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

MIB A defines: SomeDatatype ::= INTEGER(0..100)

MIB B defines: SomeDatatype ::= INTEGER(1..50)

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

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

MIB A defines: SomeDatatype ::= DisplayString

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

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

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

  1. SNMPv2-SMI.my
  2. SNMPv2-TC.my
  3. SNMPv2-MIB
  4. IF-MIB
  5. CISCO-SMI.my

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

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

Downloading MIBs

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

1. Review the considerations in the "Considerations for Working with MIBs" section.
2. Go to one of the following Cisco URLs. If the MIB you want to download is not there, try the other URL; otherwise, go to one of the URLs in Step 5.
   - ftp://ftp.cisco.com/pub/mibs/v2
   - ftp://ftp.cisco.com/pub/mibs/v1
3. Click the link for a MIB to download that MIB to your system.
4. Select **File > Save** or **File > Save As** to save the MIB on your system.
5. You can download industry-standard MIBs from the following URLs:
   - http://www.ietf.org
   - http://www.ipmplsforum.org

Compiling MIBs

If you plan to integrate the Cisco NCS 4000 Series router with an SNMP-based management application, then you must compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile Cisco NCS 4000 Series router MIBs with the HP OpenView Network Management System (NMS).

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco NCS 4000 Series router for SNMP support.

For detailed information about SNMP commands, go to the following URL:

- *Implementing SNMP* module provides general information about configuring and implementing SNMP support. It is part of the *Cisco IOS XR System Management Configuration Guide.*
- SNMP Server Commands provides information about SNMP commands. It is part of the Cisco IOS XR System Management Command Reference.

To configure the Cisco NCS 4000 Series router for SNMP support, follow these steps:

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

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

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

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

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

7. Identify (by IP address) the host to receive SNMP notifications from the router:

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

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

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

For information about how to configure SNMP community strings, refer the *SNMP Server Commands* module in the *Cisco IOS XR System Management Command Reference*.

Chapter 3 - Cisco NCS 4000 Series Routers MIB Specifications

This chapter describes the Management Information Base (MIB) on the Cisco NCS 4000 Series router. Each MIB description lists any constraints on how the MIB or its object identifiers (OIDs) are implemented on the Cisco NCS 4000 Series router.

Unless noted otherwise, the Cisco NCS 4000 Series router implementation of a MIB follows the standard MIB that has been defined. Any MIB table or object not listed in the table is implemented as defined in the standard MIB definition.

This chapter includes the following sections:

Cisco NCS 4000 Series Routers MIBs

Each MIB description lists relevant constraints about the MIB's implementation on the Cisco NCS 4000 Series router platform. Any objects not listed in a table are implemented as defined in the MIB. For detailed MIB descriptions, see the standard MIB.

Note:

- Not all MIBs included in a Cisco IOS XR 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 NCS 4000 Series Router platform.

- Certain MIBs return a numeric value along with the MIB object. These numerical values are shown in parentheses in the Cisco NCS 4000 Series Aggregation Services Routers MIB Specifications Guide. For example, the CISCO-ENHANCED-FRU-CONTROL-MIB, returns a MIB object cempMemPoolType of value processorMemory and an actual value 2. This is shown as processorMemory(2).

To determine which MIBs are included in other releases, see the "Downloading and Compiling MIBs" section on page 13.

Cisco NCS 4000 Series Routers MIB Categories

The MIBs in the Cisco NCS 4000 Series Image on the Cisco NCS 4000 Series router are categorized into two types:

- Supported MIBs
- Unsupported MIBs

Supported MIBs

The MIB exists in the image, the code is implemented.

Unsupported MIBs

The MIB exists in the image but is not supported. These MIBs are not supported for the Cisco NCS 4000 Series routers.

MIBs in the Cisco NCS 4000 Series Routers

The following table lists the MIBs in the Cisco NCS 4000 Series routers:

The following list indicates the MIBs that are supported by IOS XR on the NCS 4000 Series Router. SNMP version 1 MIBs are in the v1 directory and SNMP version 2 MIBs are in the v2 directory.

Table 1 MIBs in the Cisco NCS 4000 Series Routers

MIB	iso/pkg
CISCO-ENTITY-ASSET-MIB	ncs4k-mgbl-x.iso
CISCO-ENTITY-FRU-CONTROL-MIB	ncs4k-mgbl-x.iso
CISCO-ENTITY-SENSOR-MIB	ncs4k-mgbl-x.iso
CISCO-IF-EXTENSION-MIB	ncs4k-mini-x.iso
SONET-MIB (RFC 2558)	ncs4k-mini-x.iso
CISCO-SYSLOG-MIB	ncs4k-mini-x.iso
CISCO-SYSTEM-MIB	ncs4k-mini-x.iso
CISCO-OTN-IF-MIB	ncs4k-mini-x.iso
EtherLike-MIB	ncs4k-mini-x.iso
CISCO-FLASH-MIB	ncs4k-mini-x.iso
CISCO-IP-ADDRESS-POOL-MIB	ncs4k-mini-x.iso
MEF-SOAM-PM-MIB	ncs4k-mini-x.iso
CISCO-FABRIC-MCAST-APPL-MIB	ncs4k-mini-x.iso
IP-MIB	ncs4k-mini-x.iso
MPLS-LDP-GENERIC-STD-MIB	ncs4k-mpls.pkg
IP-FORWARD-MIB	ncs4k-mini-x.iso
UDP-MIB	ncs4k-mini-x.iso
CISCO-NTP-MIB	ncs4k-mini-x.iso
CISCO-CONFIG-MAN-MIB	ncs4k-mini-x.iso
CISCO-IETF-FRR-MIB	ncs4k-mpls.pkg
CISCO-BGP4-MIB	ncs4k-mini-x.iso
CISCO-SONET-MIB	ncs4k-mini-x.iso
CISCO-AAL5-EXT-MIB	ncs4k-mini-x.iso
CISCO-BULK-FILE-MIB	ncs4k-mgbl-x.iso
SNMP-NOTIFICATION-MIB	ncs4k-mini-x.iso
CISCO-MPLS-TE-STD-EXT-MIB	ncs4k-mpls.pkg
OSPF-MIB	ncs4k-mini-x.iso
CISCO-CDP-MIB	ncs4k-mini-x.iso
CISCO-IETF-PW-ENET-MIB	ncs4k-mpls.pkg
CISCO-SELECTIVE-VRF-DOWNLOAD-MIB	ncs4k-mini-x.iso

ISIS-MIB	ncs4k-mini-x.iso
MPLS-LDP-STD-MIB	ncs4k-mpls.pkg
EVENT-MIB	ncs4k-mini-x.iso
CISCO-IPSEC-MIB	ncs4k-k9sec.pkg
MPLS-LSR-STD-MIB	ncs4k-mpls.pkg
MPLS-L3VPN-STD-MIB	ncs4k-mini-x.iso
CISCO-HSRP-MIB	ncs4k-mini-x.iso
SNMPv2-MIB	ncs4k-mini-x.iso
CISCO-AAA-SERVER-MIB	ncs4k-mini-x.iso
CISCO-CLASS-BASED-QOS-MIB	ncs4k-mini-x.iso
CISCO-ENTITY-EXT-MIB	ncs4k-mini-x.iso
CISCO-RTTMON-MIB	ncs4k-mini-x.iso
DISMAN-EXPRESSION-MIB	ncs4k-mini-x.iso
SNMP-TARGET-MIB	ncs4k-mini-x.iso
CISCO-PROCESS-MIB	ncs4k-mini-x.iso
CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	ncs4k-mini-x.iso
IEEE8023-LAG-MIB	ncs4k-mini-x.iso
IPV6-MIB	ncs4k-mini-x.iso
OSPF-TRAP-MIB	ncs4k-mini-x.iso
CISCO-IETF-PW-MPLS-MIB	ncs4k-mini-x.iso
CISCO-IPSEC-FLOW-MONITOR-MIB	ncs4k-k9sec.pkg
CISCO-FABRIC-MCAST-MIB	ncs4k-mini-x.iso
CISCO-ENTITY-REDUNDANCY-MIB	ncs4k-mini-x.iso
CISCO-FTP-CLIENT-MIB	ncs4k-mgbl-x.iso
NOTIFICATION-LOG-MIB	ncs4k-mini-x.iso
BGP4-MIB	ncs4k-mini-x.iso
CISCO-RF-MIB	ncs4k-mini-x.iso
RSVP-MIB	ncs4k-mini-x.iso
SNMP-MPD-MIB	ncs4k-mini-x.iso
CISCO-ENHANCED-MEMPOOL-MIB	ncs4k-mgbl-x.iso
ENTITY-MIB	ncs4k-mini-x.iso
CISCO-TCP-MIB	ncs4k-mini-x.iso
CISCO-FABRIC-HFR-MIB	ncs4k-mini-x.iso
IF-MIB	ncs4k-mini-x.iso
MPLS-TE-STD-MIB	ncs4k-mpls.pkg
SNMP-FRAMEWORK-MIB	ncs4k-mini-x.iso
CISCO-IETF-PW-MIB	ncs4k-mpls.pkg
LLDP-MIB	ncs4k-mini-x.iso
TCP-MIB	ncs4k-mini-x.iso
ENTITY-STATE-MIB	ncs4k-mini-x.iso

CISCO-ENTITY-ASSET-MIB

The CISCO-ENTITY-ASSET-MIB provides asset tracking information for the physical components in the ENTITY-MIB (RFC 2737) entPhysicalTable.

The ceAssetTable contains an entry (ceAssetEntry) for each physical component on the router. Each entry provides information about the component, such as its orderable part number, serial number, hardware revision, manufacturing assembly number, and manufacturing revision.

Most physical components are programmed with a standard Cisco generic Identification Programmable Read-Only Memory (IDPROM) value that specifies asset information for the component. If possible, the MIB accesses the component's IDPROM information.

MIB Tables

The following table lists the tables in the CISCO-ENTITY-ASSET-MIB:

Table 2 CISCO-ENTITY-ASSET-MIB Tables

MIB Table	Description
ceAssetTable	Provides this information for the entities in the ENTITY-MIB entPhysicalTable: ▪ Orderable part number ▪ Serial number ▪ Hardware revision ▪ Manufacturing assembly number ▪ Revision number ▪ FirmwareID and revision if any ▪ SoftwareID and revision if any

The following table gives more information on the objects associated with this MIB:

Table 3 CISCO-ENTITY-ASSET-MIB Objects and Value Information

Name	Description
ceAssetMfgAssyNumber	Top-level assembly number stored in IDPROM
ceAssetMfgAssyRevision	This object should reflect the revision of the TAN stored in IDPROM.
ceAssetFirmwareID	This object value should be the same as entPhysicalFirmwareRev of ENTITY-MIB.
ceAssetSoftwareID	This object value should be the same as entPhysicalSoftwareRev of ENTITY-MIB.
ceAssetCLEI	This object should reflect the value of the CLEI stored in the IDPROM supported by the physical entity.

CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB contains objects to configure and monitor the operational status of field replaceable units (FRUs) on the Cisco NCS 4000 Series router listed in the ENTITY-MIB entPhysicalTable. A FRU is a hardware component (such as a line card and module, fan, or power supply) that can be replaced on site.

MIB Tables

The following table lists the tables in the CISCO-ENTTY-FRU-CONTROL-MIB:

Table 4 CISCO-ENTITY-FRU-CONTROL-MIB Tables

MIB Table	Description
cefcFRUPowerSupplyGroupTable	Displays the redundancy mode and the operational status of the power supply groups in the system.
cefcFRUPowerStatusTable	Displays the power-related administrative status and operational status of the manageable components in the system.
cefcFRUPowerSupplyValueTable	Displays the power capacity of a power FRU in the system if it provides variable power. This table supplements the information in the cefcFRUPowerStatusTable for power supply FRUs. The cefcFRUCurrent attribute in cefcFRUPowerStatusTable table indicates the type of power the FRU can supply.
cefcModuleTable	Displays the operational and administrative status information for ENTITY-MIB entPhysicalTable entries for the manageable components of type PhysicalClass module(9).
cefcIntelliModuleTable	A cefcIntelliModuleTable entry lists the information specific to intelligent modules that are not listed under the cefcModuleTable. This table supplements the cefcModuleTable (every row in this table corresponds to a row in the cefcModuleTable but not necessarily vice-versa).
cefcFanTrayStatusTable	Provides the operational status information for all the ENTITY-MIB entPhysicalTable entries that have an entPhysicalClass valus as fan. The entPhysicalClass valus as fan indicates either: ▪ A physical fan ▪ A combination of multiple fans.
cefcPhysicalTable	Displays a single row for each physical entity. Provides the power input information for all the power supplies

	that have entPhysicalTable entries with powerSupply as the entPhysicalClass.
cefcPowerSupplyOutputTable	Displays the output modes for the power supplies and the modes that are operational within the system.
cefcChassisCoolingTable	Displays the cooling capacity information of the chassis (for ENTITY-MIB entPhysicalTable entries having an entPhysicalClass value as chassis).
cefcFanCoolingTable	Displays the cooling capacity information of the fans (for ENTITY-MIB entPhysicalTable entries having an entPhysicalClass value as fanl).
cefcModuleCoolingTable	Specifies the cooling requirement for all the manageable components having entPhysicalClass value as module.
cefcFanCoolingCapTable	Displays the possible cooling capacity modes and properties of the fans(for ENTITY-MIB entPhysicalTable entries having entPhysicalClass value fan).
cefcConnectorRatingTable	Specifies the connector power ratings of FRUs.
cefcModulePowerConsumptionTable	Provides the total power consumption information for modules (for ENTITY-MIB entPhysicalTable entries having entPhysicalClass value as module).

MIB Constraints

The following table lists the constraints that the router places on objects in the CISCO-ENTITY-FRU-CONTROL-MIB:

Table 5 CISCO-ENTITY-FRU-CONTROL-MIB Constraints

MIB Object	Notes
cefcModuleTable	
cefcModuleAdminStatus	Set operation not supported
cefcModuleOperStatus	unknown (1) ok (2) failed (7)
cefcModuleResetReason	unknown (1) powerUp (2) manualReset (5)
cefcModuleLastClearConfigTime	Not implemented
cefcModuleResetReasonDescription	Not implemented
cefcModuleStateChangeReasonDescr	Not implemented
cefcFRUTotalSystemCurrent	Not supported
cefcFRUDrawnSystemCurrent	Not supported

cefcFRUTotalInlineCurrent	Not supported
cefcFRUDrawnInlineCurrent	Not supported

Table 5 CISCO-ENTITY-FRU-CONTROL-MIB Constraints (continued)

MIB Object	Notes
cefcFRUPowerAdminStatus	on(1) off(2)
cefcFRUPowerOperStatus	offEnvOther(1) on(2) offAdmin(3)
cefcPowerRedundancyMode	Not supported
cefcModuleAdminStatus	Not supported
cefcMaxDefaultHighInLinePower	Not supported
cefcFRUPowerSupplyGroupTable	Not supported
cefcFRUPowerSupplyValueTable	Not supported
cefcIntelliModuleTable	Not supported
cefcPowerSupplyInputTable	Not supported
cefcPowerSupplyOutputTable	Not supported
cefcChassisCoolingTable	Not supported
cefcFanCoolingTable	Not supported
cefcModuleCoolingTable	Not supported
cefcFanCoolingCapTable	Not supported
cefcConnectorRatingTable	Not supported
cefcModulePowerConsumptionTable	Not supported

CISCO-ENTITY-SENSOR-MIB

The CISCO-ENTITY-SENSOR-MIB contains objects to monitor the values and thresholds of sensors in the ENTITY-MIB entPhysicalTable.

MIB Tables

The following table lists the tables in CISCO-ENTITY-SENSOR-MIB:

Table 6 CISCO-ENTITY-SENSOR-MIB Tables

MIB Table	Description
entSensorValueTable	Displays the type, scale, and current value of a sensor listed in the Entity-MIB entPhysicalTable.
entSensorThresholdTable	Displays the threshold severity, relation, and comparison value for a sensor listed in the Entity-MIB entPhysicalTable.

MIB Constraints

The following table lists the constraints that the router places on the objects in the CISCO-ENTITY-SENSOR-MIB. For detailed definitions of MIB objects, see the MIB:

Table 7 CISCO-ENTITY-SENSOR-MIB Constraints

MIB Object	Notes
entSensorThresholdTable ▪ entSensorThresholdRelation ▪ entSensorThresholdSeverity ▪ entSensorThresholdValue	 Read-only Read-only Read-only

MIB Usage Values for Cisco Transceivers

The tables in this section list each type of sensor value represented in the entSensorValueTable and the entSensorThresholdTable.

The following table lists CISCO-ENTITY-SENSOR-MIB sensor objects and their usage values for Cisco NCS 4000 Series transceivers in the entSensorValueTable:

Table 8 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco Transceivers

MIB Sensor Object	Notes
Module Temperature Sensor	
▪ entSensorType	celsius (8)
▪ entSensorScale	units (9)
▪ entSensorPrecision	1
▪ entSensorStatus	ok (1)
▪ entSensorValue	Reports most recent measurement seen by the sensor
▪ entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object
▪ entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds, for example, 60 seconds.
Module Voltage Sensor	
▪ entSensorType	voltsDC(4)
▪ entSensorScale	milli (8)
▪ entSensorPrecision	1
▪ entSensorStatus	ok (1)
▪ entSensorValue	Reports most recent measurement seen by the sensor
▪ entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object
▪ entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds, for example, 60 seconds.
Tx Laser Current Sensor	
▪ entSensorType	amperes (5)
▪ entSensorScale	milli(8)
▪ entSensorPrecision	1
▪ entSensorStatus	ok (1)
▪ entSensorValue	Reports most recent measurement seen by the sensor
▪ entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object
▪ entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds, for example, 60 seconds.
Transmit Power Sensor (Optical Tx) and Receive Power Sensor (Optical Rx)	
▪ entSensorType	watts (6)
▪ entSensorScale	milli (8)
▪ entSensorPrecision	1

Table 8 CISCO-ENTITY-SENSOR-MIB Usage Values in the entSensorValueTable for Cisco Transceivers (continued)

MIB Sensor Object	Notes
▪ entSensorStatus	ok (1)
▪ entSensorValue	Reports most recent measurement seen by the sensor
▪ entSensorValueTimeStamp	Value indicates the age of the value reported by entSensorValue object
▪ entSensorValueUpdateRate	Value indicates the rate that the agent updates entSensorValue in seconds, for example, 60 seconds.

Each Cisco transceiver sensor has four threshold values corresponding to the four alarm states listed in Table 8. The entSensorValueTable is indexed by both entPhysicalIndex and entSensorThresholdIndex. The Cisco NCS 4000 Series router entSensorThresholdIndices range from 1 to 4. For N/A, a value of zero is returned.

The following table lists the default values for the Cisco transceivers in the entSensorThresholdTable:

Table 9 Default Values in the entSensorThreshold Table for Cisco Transceivers

MIB Sensor Object	High Alarm	High Warning	Low Warning	Low Alarm
Temperature	70.0	60.0	5.0	0.0
Voltage	N/A	Not applicable	Not applicable	Not applicable
Tx Bias Current	80.0	75.0	15.0	10.0
Tx Optical Power	2.0	0.9	-4.0	-9.7
Rx Optical Power	2.0	0.4	-11.9	-15.0

CISCO-IF-EXTENSION-MIB

The CISCO-IF-EXTENSION-MIB contains objects for extending the IF-MIB (RFC2863) to add objects that provide additional information about interfaces that are not available in other MIBS. This MIB replaces the OLD-CISCO-INTERFACES-MIB.

MIB Tables

The following table lists the tables in CISCO-IF-EXTENSION-MIB:

Table 10 CISCO-IF-EXTENSION-MIB Tables

Name	Description
cieIfPacketStatsTable	Displays interface packet statistics that are not listed in IF-MIB(RFC2863). These interfaces are: ▪ Ethernet ▪ FastEthernet ▪ ATM ▪ BRI ▪ Sonet ▪ GigabitEthernet
cieIfInterfaceTable	Provides extended information about interface properties that are not available in IF-MIB (RFC 2863).
cieIfStatusListTable	Provides information such as ifIndex, interface operational mode, and interface operational cause for all the interfaces in modules. The table contains individual entries for all the 64 interfaces in a module.
cieIfDot1qCustomEtherTypeTable	Displays the interfaces that support the 802.1q custom Ethertype feature.
cieIfUtilTable	Displays the interface utilization rates for inbound and outbound traffic on an interface. The cieIfInOctetRate object and cieIfOutOctetRate object are used for reporting number of bytes of data transferred from/to an interface in a given time period.
cieIfDot1dBaseMappingTable	Contains the mappings between ifIndex of an interface to its corresponding dot1dBasePort value.
cieIfNameMappingTable	Provides mapping information between ifName and ifIndex. This table contains an entry for each valid ifName available in the system.

MIB Constraints

The following table lists the constraints on objects in the CISCO-IF-EXTENSION-MIB:

Table 11 CISCO-IF-EXTENSION-MIB Constraints

MIB Object	Notes
cieSystemMtu	Not supported
cieIfDot1qCustomAdminEtherType	Not supported
cieLinkUpDownEnable	Not supported
cieStandardLinkUpDownVarbinds	Not supported
cieIfDhcpMode	Not supported
cieIfMtu	Not supported
cieIfAutoNegotiate	Not supported
cieIfKeepAliveEnabled	Not supported
cieIfLastInTime	Not supported
cieIfLastOutTime	Not supported
cieIfLastOutHangTime	Not supported
cieIfPacketDiscontinuityTime	Not supported
cieIfStatusListIndex	Not supported
cieInterfaceOwnershipBitmap	Not supported
cieIfInterfaceDiscontinuityTime	Not supported
CieIfVlStatsEntry	Not supported
cieIfNoDropVlInPkts	Not supported
cieIfNoDropVlInOctets	Not supported
cieIfNoDropVlOutPkts	Not supported
cieIfNoDropVlOutOctets	Not supported
cieIfDropVlInPkts	Not supported
cieIfDropVlInOctets	Not supported
cieIfDropVlOutPkts	Not supported
cieIfDropVlOutOctets	Not supported
cieIfIndexPersistence	Not supported
cieIfIndexPersistenceEnabled	Not supported
cieIfIndexPersistenceControl	Not supported
cieDelayedLinkUpDownNotifEnable	Not supported
cieDelayedLinkUpDownNotifDelay	Not supported
cieIfIndexGlobalPersistence	Not supported
cieLinkUpDownConfig	Not supported
cieIfSpeedReceive	Not supported
cieIfHighSpeedReceive	Not supported
cieIfOwner	Not supported

CISCO-OTN-IF-MIB

The CISCO-OTN-IF-MIB defines the managed objects for physical layer characteristics of DWDM optical channel interfaces and performance statistics objects for protocol specific error counters in DWDM optical devices.

Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for and report performance data for early detection of problems. Thresholds are used to set error levels for each PM parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alarm (TCA) is generated. The TCAs provide early detection of performance degradation.

MIB Objects

The following table lists the tables associated with this MIB:

Table 12 CISCO-OTN-IF-MIB Tables and Descriptions

Name	Description
coiIfControllerTable	This table provides management information for physical layer related attributes of interfaces with an ifType of opticalChannel (195).
coiOtnNearEndThresholdsTable	This table provides objects for configuring OTN (G.709) near end error thresholds on interfaces of ifType opticalChannel (195).
coiOtnFarEndThresholdsTable	This table provides objects for configuring OTN (G.709) thresholds for far end of interfaces of ifType opticalChannel (195).
coiOtnNearEndCurrentTable	This table contains the cumulative OTN (G.709) PM statistics for the near end of interfaces of ifType opticalChannel (195). The statistics are for the current interval of interval type identified by coiOtnNearEndCurIntervalType. The current PM statistics is the accumulated statistics for the time period defined by the interval type.
coiOtnFarEndCurrentTable	This table contains the cumulative OTN (G.709) PM stats for the far end of interfaces of ifType opticalChannel (195). The statistics are for the current interval of interval type identified by coiOtnFarEndCurIntervalType. The current PM statistics is the accumulated statistics for the time period defined by the interval type.
coiOtnNearEndIntervalTable	This table contains historical cumulative OTN (G.709) PM stats for the near end of interfaces of ifType opticalChannel (195), for the interval type identified by the index coiOtnNearEndIntervalType and the interval number as identified by the index coiOtnNearEndIntervalNum. The PM statistics is the accumulated stats for the time period defined by the interval type in the time interval as defined by interval number.

Table 12 CISCO-OTN-IF-MIB Tables and Descriptions (continued)

Name	Description
coiOtnFarEndIntervalTable	This table contains historical cumulative OTN (G.709) PM stats for the far end interfaces of ifType opticalChannel (195), for the interval type identified by the index coiOtnFarEndIntervalType and the interval number as identified by coiOtnFarEndIntervalNum. The PM statistics is the accumulated stats for the time period defined by the interval type in the time interval as defined by interval number.
coiFECThresholdsTable	This table contains the configurable thresholds for Forward Error Correction statistics.
coiFECCurrentTable	This table contains the cumulative FEC PM stats for the interfaces of ifType opticalChannel (195) for the current interval of interval type identified coiFECCurIntervalType.
coiFECIntervalTable	This table contains historical cumulative FEC PM stats for the interfaces of ifType opticalChannel (195), for the interval type identified by the index coiFECIntervalType and the interval number as identified by index coiFECIntervalNum. The PM statistics is the accumulated stats for the time period defined by the interval type in the time interval as defined by interval number.

SONET-MIB (RFC 2558)

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

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

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

Note: The intervals in a dsx1IntervalTable are reset during an OIR operation whereas the SONET intervals are not reset.

MIB Tables

The following table lists the tables in SONET-MIB:

Table 13 SONET-MIB Tables

MIB Table	Description
sonetMediumTable	The SONET/SDH Medium table.
sonetSectionCurrentTable	The SONET/SDH Section Current table
sonetSectionIntervalTable	The SONET/SDH Section Interval table.
sonetLineCurrentTable	The SONET/SDH Line Current table.
sonetLineIntervalTable	The SONET/SDH Line Interval table.
sonetFarEndLineCurrentTable	The SONET/SDH Far End Line Current table.
sonetFarEndLineIntervalTable	The SONET/SDH Far End Line Interval table.
sonetPathCurrentTable	The SONET/SDH Path Current table.
sonetPathIntervalTable	The SONET/SDH Path Interval table.
sonetFarEndPathCurrentTable	The SONET/SDH Far End Path Current table.
sonetFarEndPathIntervalTable	The SONET/SDH Far End Path Interval table.
sonetVTCurrentTable	The SONET/SDH VT Current table.
sonetVTIntervalTable	The SONET/SDH VT Interval table.
sonetFarEndVTCurrentTable	The SONET/SDH Far End VT Current table.
sonetFarEndVTIntervalTable	The SONET/SDH Far End VT Interval table.

MIB Constraints

The following table lists the constraints that the NCS 4000 Series router places on objects in the Sonet-MIB(RFC 2558):

Table 14 Sonet-MIB Constraints

MIB Object	Notes
sonetPathCurrentTable	
▪ sonetPathCurrentWidth	Read-only
sonetVTCurrentTable	Not Implemented

Table 14 Sonet-MIB Constraints (continued)

MIB Object	Notes
sonetVTIntervalTable	Not Implemented
sonetFarEndVTCurrentTable	Not Implemented
sonetFarEndVTIntervalTable	Not Implemented
SonetMediumTable	
▪ sonetMediumLineCoding	Read-only
▪ sonetMediumLineType	Read-only
▪ sonetMediumCircuitIdentifier	Read-only
▪ sonetMediumLoopbackConfig	Read-only
sonetSESthresholdSet	Not Implemented

TCP-MIB

The TCP-MIB is the MIB module for managing TCP implementations.

The following table lists the tables associated with this MIB:

Table 15 TCP-MIB Tables and Descriptions

Name	Description
tcpConnectionTable	Table containing information about existing TCP connections. Note:that unlike earlier TCP MIBs, there is a separate table for connections in the LISTEN state
tcpListenerTable	Table containing information about TCP listeners. A listening application can be represented in three possible ways: 1. An application that is willing to accept both IPv4 and IPv6 datagrams is represented by a tcpListenerLocalAddressType of unknown (0) and a tcpListenerLocalAddress of 'h' (a zero-length octet-string). 2. An application that is willing to accept only IPv4 or IPv6 datagrams is represented by a tcpListenerLocalAddressType of the appropriate address type and a tcpListenerLocalAddress of '0.0.0.0' or '::' respectively. 3. An application that is listening for data destined only to a specific IP address, but from any remote system, is represented by a tcpListenerLocalAddressType of an appropriate address type, with tcpListenerLocalAddress as the specific local address. **Note** The address type in this table represents the address type used for the communication, irrespective of the higher-layer abstraction. For example, an application using IPv6 'sockets' to communicate via IPv4 between ::ffff:10.0.0.1 and ::ffff:10.0.0.2 would use InetAddressType IPv4(1))
tcpConnTable	Table containing information about existing IPv4-specific TCP connections or listeners. This table has been deprecated in favor of the version neutral tcpConnectionTable

MIB Constraints

The following table lists the constraints that the router places on objects in the TCP-MIB:

Table 16 TCP-MIB Constraints

MIB Object	Notes
tcpConnectionTable	
tcpConnectionProcess	Not supported

OSPFV3-MIB

The OSPFV3-MIB is the MIB module for OSPF version 3.

The following table lists the tables associated with this MIB:

Table 17 OSPFV3-MIB Tables and Descriptions

Name	Description
ospfv3AreaTable	OSPFv3 Process's AS-Scope LSDB. The LSDB contains the AS-Scope Link State Advertisements from throughout the areas that the device is attached to.
ospfv3AsLsdbTable	OSPFv3 Process's AS-Scope LSDB. The LSDB contains the AS-Scope Link State Advertisements from throughout the areas that the device is attached to.
ospfv3AreaLsdbTable	OSPFv3 Process's Area-Scope LSDB. The LSDB contains the Area-Scope Link State Advertisements from throughout the area that the device is attached to.
ospfv3LinkLsdbTable	OSPFv3 Process's Link-Scope LSDB for non-virtual interfaces. The LSDB contains the Link-Scope Link State Advertisements from the interfaces that the device is attached to
ospfv3HostTable	Host/Metric Table indicates what hosts are directly attached to the router and their corresponding metrics
ospfv3IfTable	OSPFv3 Interface Table describes the interfaces from the viewpoint of OSPFv3
ospfv3VirtIfTable	Information about this router's virtual interfaces that the OSPFv3 Process is configured to carry on
ospfv3NbrTable	A table describing all neighbors in the locality of the OSPFv3 router
ospfv3CfgNbrTable	Table describing all configured neighbors
ospfv3VirtNbrTable	Table describing all virtual neighbors

Table 17 OSPFV3-MIB Tables and Descriptions (continued)

MIB Object	Notes
ospfv3AreaAggregateTable	Area Aggregate Table acts as an adjunct to the Area Table. It describes those address aggregates that are configured to be propagated from an area. Its purpose is to reduce the amount of information that is known beyond an Area's borders. A range of IPv6 prefixes specified by a prefix/prefix length pair. Note that if ranges are configured such that one range subsumes another range the most specific match is the preferred one.
ospfv3VirtLinkLsdbTable	OSPFv3 Process's Link-Scope LSDB for virtual interfaces. The LSDB contains the Link-Scope Link State Advertisements from virtual interfaces

MIB Constraints

The following table lists the constraints on objects in the OSPFV3-MIB:

Table 18 OSPFV3-MIB Constraints

MIB Object	Notes
ospfv3RouterId	Not supported
ospfv3AdminStat	Not supported
ospfv3ASBdrRtrStatus	Not supported
ospfv3ExtAreaLsdbLimit	Not supported
ospfv3MulticastExtensions	Not supported
ospfv3ExitOverflowInterval	Not supported
ospfv3DemandExtensions	Not supported
ospfv3TrafficEngineeringSupport	Not supported
ospfv3ReferenceBandwidth	Not supported
ospfv3RestartSupport	Not supported
ospfv3RestartInterval	Not supported
ospfv3ImportAsExtern	Not supported
ospfv3AreaSummary	Not supported
ospfv3AreaStatus	Not supported
ospfv3StubMetric	Not supported
ospfv3AreaNssaTranslatorRole	Not supported
ospfv3AreaNssaTranslatorStabilityInterval	Not supported
ospfv3AreaStubMetricType	Not supported
ospfv3NbmaNbrPriority	Not supported
ospfv3NbmaNbrStorageType	Not supported
ospfv3NbmaNbrStatus	Not supported
ospfv3VirtIfIndex	Not supported
ospfv3VirtIfTransitDelay	Not supported
ospfv3VirtIfRetransInterval	Not supported

ospfv3VirtIfHelloInterval	Not supported

Table 18 OSPFV3-MIB Constraints (continued)

MIB Object	Notes
ospfv3VirtIfRtrDeadInterval	Not supported
ospfv3VirtIfStatus	Not supported
ospfv3AreaAggregateStatus	Not supported
ospfv3AreaAggregateEffect	Not supported
ospfv3AreaAggregateRouteTag	Not supported
ospfv3IfAreaId	Not supported
ospfv3IfType	Not supported
ospfv3IfAdminStat	Not supported
ospfv3IfRtrPriority	Not supported
ospfv3IfTransitDelay	Not supported
ospfv3IfRetransInterval	Not supported
ospfv3IfHelloInterval	Not supported
ospfv3IfRtrDeadInterval	Not supported
ospfv3IfPollInterval	Not supported
ospfv3IfStatus	Not supported
ospfv3IfMulticastForwarding	Not supported
ospfv3IfDemand	Not supported
ospfv3IfMetricValue	Not supported
ospfv3IfInstId	Not supported
ospfv3IfDemandNbrProbe	Not supported
ospfv3IfDemandNbrProbeRetxLimit	Not supported
ospfv3IfDemandNbrProbeInterval	Not supported
ospfv3HostMetric	Not supported
ospfv3HostStatus	Not supported
ospfv3HostAreaID	Not supported

CISCO-SYSLOG-MIB

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

Note: You can configure the Cisco NCS 4000 Series router to send syslog messages to a syslog server.

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

The following table lists the tables associated with this MIB:

Table 19 CISCO-SYSLOG-MIB Tables and Descriptions

Name	Description
clogHistoryTable	Table of syslog messages generated by this device. All 'interesting' syslog messages (that is, severity <= clogMaxSeverity) are entered into this table.
clogServerConfigTable	This table contains entries that allow application to configure syslog servers for the system. The maximum number of entries that can be created for this table is limited by the object clogMaxServers.

MIB Constraints

The following table lists the constraints on objects in the CISCO-SYSLOG-MIB:

Table 20 CISCO-SYSLOG-MIB Constraints

MIB Object	Notes
clogServerMaxTable	Not supported

CISCO-SYSTEM-MIB

The CISCO-SYSTEM-MIB provides a standard set of basic system information. This MIB module contains Cisco-defined extensions to the systemGroup. This MIB has no tables.

CISCO-TCP-MIB

An extension to the IETF MIB module for managing TCP implementations

CISCO-FLASH-MIB

This MIB provides for the management of Cisco Flash Devices

CISCO-CDP-MIB

SNMP-COMMUNITY-MIB (RFC 2576)

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

The following table lists the tables associated with this MIB:

Table 21 SNMP-COMMUNITY-MIB Tables and Descriptions

Name	Description
snmpCommunityTable	Table of community strings configured in the SNMP engine's LCD.
snmpTargetAddrExtTable	Table of mask and mms values associated with the snmpTargetAddrTable. The snmpTargetAddrExtTable augments the snmpTargetAddrTable with a transport address mask value and a maximum message size value. The transport address mask allows entries in the snmpTargetAddrTable to define a set of addresses instead of just a single address. The maximum message size value allows the maximum message size of another SNMP entity to be configured for use in SNMPv1 (and SNMPv2c) transactions, where the message format does not specify a maximum message size.

CISCO-IP-ADDRESS-POOL-MIB

This MIB modules defines objects that describe common aspects of IP address pools.
IP Address Pool Manager: The IP address pool manager consists of the software that maintains IP address pools and supports the following capabilities:

- Create an IP address pool group.
- Destroy an IP address pool group.
- Create an IP address pool and add it to an IP address pool group.
- Remove an IP address pool from an IP address pool group and destroy it.
- Create a range of IP addresses and add it to an IP address pool.
- Remove a range of IP addresses from an IP address pool and destroy it.
- Allocate an IP address from an IP address pool.
- Return a previously allocated IP address to the IP address pool that it was allocated from.
- Create a set of IP prefixes and adding it to an IP address pool.
- Remove a set of IP prefixes from an IP address pool and destroy it.
- Allocate an IP prefix from an IP address pool.
- Return a previously allocated IP prefix to the IP address pool that it was allocated from.

IP Address Pool: An IP address pool consists of a collection of IP addresses from which a client (e.g., PPP or DHCP) can allocate an IP address for the purpose of assigning it to a remote peer. This collection consists of a one or more range of IP addresses. Observe that human interfaces allow a user to specify ranges of IP addresses using a variety of means to simplify the process. For example, a human interface may simply allow a user to specify a subnet. No matter what abstraction a human interface employs, the end result is always one or more range of IP addresses. Thus, this MIB module abstracts an IP address pool as one or more range of IP addresses. This places the burden on any application employing other abstractions to transform to the abstraction defined by this MIB module. Alternatively, an IP address pool can also consist of a collection of IP prefixes from which a client can allocate an IP prefix for the purpose of assigning it to a remote peer. This collection consists of one or more set of IP prefixes. Observe that the term 'IP prefix' here can refer to an IPv4 subnet or an IPv6 prefix.

IP Address Pool Group: An IP address pool group contains the IP address pools belonging to the same administrative domain. Examples of administrative domains include a Virtual Route Forwarding (VRF) instance and a Virtual Private Network (VPN). Observe that the IP addresses contained by the IP address pools in two distinct IP address pool groups

may overlap.

IP Address Pool Threshold Monitoring: An IP address pool manager maintains a number of gauges for the purpose of monitoring the number of allocated IP addresses. We refer to these gauges as 'in-use gauges'. Each in-use gauge has a corresponding state that can have one of two values:

9. Off The IP address pool manager monitors the number of allocated addresses or prefixes. If this value is greater than the configured rising threshold and the previous value was less than or equal to the same rising threshold, then the IP address manager transitions the state to 'On'.

10. On The IP address pool manager monitors the number of allocated addresses or prefixes. If the value is less than the configured falling threshold and the previous value was greater than or equal to the same falling threshold, then the IP address manager transitions the state to 'Off'. Observe that while the values of the configured rising and falling thresholds may be the same, this may result in undesirable behavior (i.e., the IP address pool manager may generate more threshold crossing notifications than desirable).

The IP address pool manager only generates threshold crossing notifications when it transitions the corresponding state of an in-use gauge and the value of ciapGlobalNotifyEnable is 'true'. The IP address pool manager may maintain in-use gauges for the following:

- A range of IP addresses comprising an IP address pool
- A set of IP prefixes comprising an IP address pool
- An IP address pool - An IP address pool group

Observe that the IP address pool manager must initialize the state of each in-use gauge to 'Off' for threshold monitoring to operate in the prescribed manner.

MIB Objects

Table 22 CISCO-IP-ADDRESS-POOL-MIB Tables and Descriptions

Name	Description
ciapPoolTable	This table lists the IP address pools maintained by the IP address pool manager.
ciapRangeTable	This table lists the ranges of IP addresses contained by each IP address pool maintained by the IP address pool manager.
ciapPrefixTable	This table lists the IP prefixes contained by each IP address pool maintained by the IP address pool manager.
ciapPoolGroupTable	This table lists the IP address pool groups maintained by the IP address pool manager.
ciapPoolGroupContainsTable	This table lists the IP address pools contained by each IP address pool group maintained by the IP address pool manager.
ciapAllocatedAddressTable	This table lists of the IP addresses, IPv4 subnets, and IPv6 prefixes allocated from the IP address pools maintained by the IP address pool manager.

MIB Constraints

The following table lists the constraints on objects in the CISCO-IP-ADDRESS-POOL-MIB:

Table 23 CISCO-IP-ADDRESS-POOL-MIB Constraints

MIB Object	Notes
Global Objects	Not-supported
ciapGlobalNotifyEnable	Not-supported
ciapGlobalThresholdUnits	Not-supported
ciapGlobalThresholdRising	Not-supported
ciapGlobalThresholdFalling	Not-supported

Table 23 CISCO-IP-ADDRESS-POOL-MIB Constraints (continued)

MIB Object	Notes
ciapPoolIdNext	Supported
Pool Table Objects	
ciapPoolStatus	Supported
ciapPoolStorage	Not-supported
ciapPoolName	Supported
ciapPoolType	Supported
ciapPoolContainedIn	Supported
ciapPoolThresholdUnits	Supported
ciapPoolThresholdRising	Supported
ciapPoolThresholdFalling	Supported
ciapPoolAddressesInUse	Supported
ciapPoolAddressesFree	Supported
ciapPoolTableChanged	Not-supported
Pool Address Range Objects	
ciapRangeStatus	Supported
ciapRangeStorage	Not-supported
ciapRangeAddressUpper	Supported
ciapRangeCacheSize	Not-supported
ciapRangeRecycleDelay	Not-supported
ciapRangePriority	Not-supported
ciapRangeThresholdUnits	Not-supported
ciapRangeThresholdRising	Not-supported
ciapRangeThresholdFalling	Not-supported
ciapRangeAddressesInUse	Supported
ciapRangeAddressesFree	Supported
ciapRangeTableChanged	Not-supported
Pool Prefix Range Objects (applicable only for IPv6 prefixes)	
ciapPrefixStatus	Supported
ciapPrefixStorage	Not-supported
ciapPrefixAssignedLength	Supported
ciapPrefixCacheSize	Not-supported
ciapPrefixRecycleDelay	Not-supported
ciapPrefixPriority	Not-supported
ciapPrefixThresholdUnits	Not-supported
ciapPrefixThresholdRising	Not-supported

Table 23 CISCO-IP-ADDRESS-POOL-MIB Constraints (continued)

MIB Object	Notes
ciapPrefixThresholdFalling	Not-supported
ciapPrefixPrefixesInUse	Supported
ciapPrefixPrefixesFree	Supported
ciapPrefixTableChanged	Not-supported
ciapPoolGroupIdNext	Supported
Pool Group (VRF) Related Objects	
ciapPoolGroupName	Supported
ciapPoolGroupThresholdUnits	Not-supported
ciapPoolGroupThresholdRising	Not-supported
ciapPoolGroupThresholdFalling	Not-supported
ciapPoolGroupAddressesInUse	Supported
ciapPoolGroupAddressesFree	Supported
ciapPoolGroupContainsId	Supported
Allocated Address Objects	
ciapAllocatedAddressMask	Not-supported
Notification Objects	
ciapNotifyResource	Supported
ciapNotifyThresholdUnits	Supported
ciapNotifyThresholdRising	Supported
ciapNotifyThresholdFalling	Supported
ciapNotifyInUse	Supported
ciapNotifyFree	Supported
ciapEventThresholdRising	Supported
ciapEventThresholdFalling	Supported

CISCO-FABRIC-MCAST-MIB

This MIB module is used for managing/tracking the fabric multicast resource related information.

SNMP-FRAMEWORK-MIB (RFC 2571)

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

SNMP-NOTIFICATION-MIB (RFC 2573)

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

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

SNMP-TARGET-MIB (RFC 2573)

The SNMP-TARGET-MIB (RFC 2573) contains objects to remotely configure the parameters used by an entity to generate SNMP notifications. The MIB defines the addresses of the destination entities for SNMP notifications and contains a list of tag values that are used to filter the notifications sent to the entities (see the SNMP-NOTIFICATION-MIB). There are no constraints on this MIB.

The following table lists the tables associated with this MIB:

Table 24 SNMP-TARGET-MIB Tables and Descriptions

Name	Description
snmpTargetAddrTable	Table of transport addresses to be used in the generation of SNMP messages
snmpTargetParamsTable	Table of SNMP target information to be used in the generation of SNMP messages

SNMP-USM-MIB (RFC 2574)

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

SNMPv2-MIB (RFC 1907)

The SNMPv2-MIB contains objects SNMPv2 entities. The SNMPv2-MIB contains the following mandatory object groups:

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

SNMP-VACM-MIB

The SNMP-VACM-MIB contains objects to manage the View-Based Access Control Model (VACM) for SNMP clients and managers. 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).

BGP4-MIB

The MIB module for BGP-4.

The following table lists the tables associated with this MIB:

MIB Name	Description
bgp4PathAttrAggregatorAddr	" The IP address of the last BGP4 speaker that performed route aggregation. A value of 0.0.0.0 indicates the absence of this attribute."
bgp4PathAttrAggregatorAS	" The AS number of the last BGP4 speaker that performed route aggregation. A value of zero (0) indicates the absence of this attribute."
bgp4PathAttrASPathSegment	" The sequence of AS path segments. Each AS path segment is represented by a triple . The type is a 1-octet field which has two possible values: 1 AS_SET: unordered set of ASs a route in the UPDATE message has traversed 2 AS_SEQUENCE: ordered set of ASs a route in the UPDATE message has traversed. The length is a 1-octet field containing the number of ASs in the value field. The value field contains one or more AS numbers, each AS is represented in the octet string as a pair of octets according to the following algorithm: first-byte-of-pair = ASNumber / 256; second-byte-of-pair = ASNumber & 255;"
bgp4PathAttrAtomicAggregate	" Whether or not the local system has selected a less specific route without selecting a more specific route."
bgp4PathAttrBest	" An indication of whether or not this route was chosen as the best BGP4 route."
bgp4PathAttrCalcLocalPref	" The degree of preference calculated by the receiving BGP4 speaker for an advertised route. A value of -1 indicates the absence of this attribute."
bgp4PathAttrIpAddrPrefix	" An IP address prefix in the Network Layer Reachability Information field. This object is an IP address containing the prefix with length specified by bgp4PathAttrIpAddrPrefixLen. Any bits beyond the length specified by bgp4PathAttrIpAddrPrefixLen are zeroed."
bgp4PathAttrIpAddrPrefixLen	" Length in bits of the IP address prefix in the Network Layer Reachability Information field."
bgp4PathAttrLocalPref	" The originating BGP4 speaker's degree of preference for an advertised route. A value of -1 indicates the absence of this attribute."
bgp4PathAttrMultiExitDisc	" This metric is used to discriminate between multiple exit points to an adjacent autonomous system. A value of -1 indicates the absence of this attribute."
bgp4PathAttrNextHop	" The address of the border router that should be used for the destination network."
bgp4PathAttrOrigin	" The ultimate origin of the path information."
bgp4PathAttrPeer	" The IP address of the peer where the path information was learned."

bgp4PathAttrUnknown	" One or more path attributes not understood by this BGP4 speaker. Size zero (0) indicates the absence of such attribute(s). Octets beyond the maximum size, if any, are not recorded by this object."
bgpIdentifier	" The BGP Identifier of local system."
bgpLocalAs	" The local autonomous system number."
bgpPeerAdminStatus	" The desired state of the BGP connection. A transition from 'stop' to 'start' will cause the BGP Start Event to be generated. A transition from 'start' to 'stop' will cause the BGP Stop Event to be generated. This parameter can be used to restart BGP peer connections. Care should be used in providing write access to this object without adequate authentication."
bgpPeerConnectRetryInterval	" Time interval in seconds for the ConnectRetry timer. The suggested value for this timer is 120 seconds."
bgpPeerFsmEstablishedTime	" This timer indicates how long (in seconds) this peer has been in the Established state or how long since this peer was last in the Established state. It is set to zero when a new peer is configured or the router is booted."
bgpPeerFsmEstablishedTransitions	" The total number of times the BGP FSM transitioned into the established state."
bgpPeerHoldTime	" Time interval in seconds for the Hold Timer established with the peer. The value of this object is calculated by this BGP speaker by using the smaller of the value in bgpPeerHoldTimeConfigured and the Hold Time received in the OPEN message. This value must be at lease three seconds if it is not zero (0) in which case the Hold Timer has not been established with the peer, or, the value of bgpPeerHoldTimeConfigured is zero (0)."
bgpPeerHoldTimeConfigured	" Time interval in seconds for the Hold Time configured for this BGP speaker with this peer. This value is placed in an OPEN message sent to this peer by this BGP speaker, and is compared with the Hold Time field in an OPEN message received from the peer when determining the Hold Time (bgpPeerHoldTime) with the peer. This value must not be less than three seconds if it is not zero (0) in which case the Hold Time is NOT to be established with the peer. The suggested value for this timer is 90 seconds."
bgpPeerIdentifier	" The BGP Identifier of this entry's BGP peer."
bgpPeerInTotalMessages	" The total number of messages received from the remote peer on this connection. This object should be initialized to zero when the connection is established."

bgpPeerInUpdateElapsedTime	" Elapsed time in seconds since the last BGP UPDATE message was received from the peer. Each time bgpPeerInUpdates is incremented, the value of this object is set to zero (0)."
bgpPeerInUpdates	" The number of BGP UPDATE messages received on this connection. This object should be initialized to zero (0) when the connection is established."
bgpPeerKeepAlive	" Time interval in seconds for the KeepAlive timer established with the peer. The value of this object is calculated by this BGP speaker such that, when compared with bgpPeerHoldTime, it has the same proportion as what bgpPeerKeepAliveConfigured has when compared with bgpPeerHoldTimeConfigured. If the value of this object is zero (0), it indicates that the KeepAlive timer has not been established with the peer, or, the value of bgpPeerKeepAliveConfigured is zero (0)."
bgpPeerKeepAliveConfigured	" Time interval in seconds for the KeepAlive timer configured for this BGP speaker with this peer. The value of this object will only determine the KEEPALIVE messages' frequency relative to the value specified in bgpPeerHoldTimeConfigured; the actual time interval for the KEEPALIVE messages is indicated by bgpPeerKeepAlive. A reasonable maximum value for this timer would be configured to be one third of that of bgpPeerHoldTimeConfigured. If the value of this object is zero (0), no periodical KEEPALIVE messages are sent to the peer after the BGP connection has been established. The suggested value for this timer is 30 seconds."
bgpPeerLastError	" The last error code and subcode seen by this peer on this connection. If no error has occurred, this field is zero. Otherwise, the first byte of this two byte OCTET STRING contains the error code, and the second byte contains the subcode."
bgpPeerLocalAddr	" The local IP address of this entry's BGP connection."
bgpPeerLocalPort	" The local port for the TCP connection between the BGP peers."
bgpPeerMinASOriginationInterval	" Time interval in seconds for the MinASOriginationInterval timer. The suggested value for this timer is 15 seconds."
bgpPeerMinRouteAdvertisementInterval	" Time interval in seconds for the MinRouteAdvertisementInterval timer. The suggested value for this timer is 30 seconds."
bgpPeerNegotiatedVersion	" The negotiated version of BGP running between the two peers."

bgpPeerOutTotalMessages	" The total number of messages transmitted to the remote peer on this connection. This object should be initialized to zero when the connection is established."
bgpPeerOutUpdates	" The number of BGP UPDATE messages transmitted on this connection. This object should be initialized to zero (0) when the connection is established."
bgpPeerRemoteAddr	" The remote IP address of this entry's BGP peer."
bgpPeerRemoteAs	" The remote autonomous system number."
bgpPeerRemotePort	" The remote port for the TCP connection between the BGP peers. Note that the objects bgpPeerLocalAddr, bgpPeerLocalPort, bgpPeerRemoteAddr and bgpPeerRemotePort provide the appropriate reference to the standard MIB TCP connection table."
bgpPeerState	" The BGP peer connection state."
bgpVersion	" Vector of supported BGP protocol version numbers. Each peer negotiates the version from this vector. Versions are identified via the string of bits contained within this object. The first octet contains bits 0 to 7, the second octet contains bits 8 to 15, and so on, with the most significant bit referring to the lowest bit number in the octet (e.g., the MSB of the first octet refers to bit 0). If a bit, i, is present and set, then the version (i+1) of the BGP is supported."
CISCO-AAA-SERVER-MIB	" The MIB module for monitoring communications and status of AAA Server operation "
casServerStateChangeEnable	" This variable controls the generation of casServerStateChange notification. When this variable is true(1), generation of casServerStateChange notifications is enabled. When this variable is false(2), generation of casServerStateChange notifications is disabled. The default value is false(2). "
CISCO-BULK-FILE-MIB	" The MIB module for creating and deleting bulk files of SNMP data for file transfer."
cbfDefineFiles	" The current number of file definitions in cbfDefineFileTable."
cbfDefineFilesRefused	" The number of attempts to create a file definition that failed due to exceeding cbfDefineMaxFiles."
cbfDefineHighFiles	" The maximum value of cbfDefineFiles since system initialization."
cbfDefineHighObjects	" The maximum value of cbfDefineObjects since system initialization."

cbfDefineMaxFiles	" The maximum number of file definitions this system can hold in cbfDefineFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number does not disturb existing entries."
cbfDefineMaxObjects	" The maximum total number of object selections to go with file definitions this system, that is, the total number of objects this system can hold in cbfDefineObjectTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number does not disturb existing entries."
cbfDefineObjects	" The current number of object selections in cbfDefineObjectTable."
cbfDefineObjectsRefused	" The number of attempts to create an object selection that failed due to exceeding cbfDefineMaxObjects."
cbfStatusFiles	" The current number of file statuses in cbfStatusFileTable."
cbfStatusFilesBumped	" The number times the oldest entry was deleted due to exceeding cbfStatusMaxFiles."
cbfStatusHighFiles	" The maximum value of cbfStatusFiles since system initialization."
cbfStatusMaxFiles	" The maximum number of file statuses this system can hold in cbfStatusFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number deletes the oldest finished entries until the new limit is satisfied."

CISCO-BGP4-MIB

An extension to the IETF BGP4 MIB module defined in RFC 1657. Following is the terminology associated with Border Gateway Protocol(BGP). UPDATE message UPDATE messages are used to transfer routing information between BGP peers. An UPDATE message is used to advertise a single feasible route to a peer, or to withdraw multiple unfeasible routes from service. Adj-RIBs-In The Adj-RIBs-In store routing information that has been learned from inbound UPDATE messages. Their contents represent routes that are available as an input to the Decision Process. Loc-RIB(BGP table) The Loc-RIB contains the local routing information that the BGP speaker has selected by applying its local policies to the routing information contained in its Adj-RIBs-In. Adj-RIBs-Out The Adj-RIBs-Out store the information that the local BGP speaker has selected for advertisement to its peers. The routing information stored in the Adj-RIBs-Out will be carried in the local BGP speaker's UPDATE messages and advertised to its peers. Path Attributes A variable length sequence of path attributes is present in every UPDATE. Each path attribute is a triple of variable length. Network Layer Reachability Information(NLRI) A variable length field present in UPDATE messages which contains a list of Network Layer address prefixes. Address Family Identifier(AFI) Primary identifier to indicate the type of the Network Layer Reachability Information(NLRI) being carried. Subsequent Address Family Identifier(SAFI) Secondary identifier to indicate the type of the Network Layer Reachability Information(NLRI) being carried.

The following table lists the tables associated with this MIB:

MIB Name	Description
cbgpLocalAs	" The local autonomous system (AS) number." REFERENCE " RFC 4271, Section 4.2, 'My Autonomous System'. RFC 4893, BGP Support for Four-octet AS Number Space."
cbgpNotifsEnable	" Indicates whether the specific notifications are enabled. If notifsEnable(0) bit is set to 1, then the notifications defined in ciscoBgp4NotificationsGroup1 are enabled; If notifsPeer2Enable(1) bit is set to 1, then the notifications defined in ciscoBgp4Peer2NotificationsGroup are enabled."
cbgpPeer2AdminStatus	" The desired state of the BGP connection. A transition from 'stop' to 'start' will cause the BGP Manual Start Event to be generated. A transition from 'start' to 'stop' will cause the BGP Manual Stop Event to be generated. This parameter can be used to restart BGP peer connections. Care should be used in providing write access to this object without adequate authentication." REFERENCE " RFC 4271, Section 8.1.2."

cbgpPeer2CapValue	" The value of the announced capability.REFERENCE " RFC 2842, Capabilities Advertisement with BGP-4. RFC 2818, Route Refresh Capability for BGP-4. RFC 2858, Multiprotocol Extensions for BGP-4. RFC 4724, Graceful Restart Mechanism for BGP. RFC 4893, BGP Support for Four-octet AS Number Space. draft-ietf-idr-add-paths-04.txt, Advertisement of Multiple Paths in BGP."
cbgpPeer2ConnectRetryInterval	" Time interval (in seconds) for the ConnectRetry timer. The suggested value for this timer is 120 seconds." REFERENCE " RFC 4271, Section 8.2.2. This is the value used to initialize the 'ConnectRetryTimer'."
cbgpPeer2FsmEstablishedTime	" This timer indicates how long (in seconds) this peer has been in the established state or how long since this peer was last in the established state. It is set to zero when a new peer is configured or when the router is booted." REFERENCE " RFC 4271, Section 8."
cbgpPeer2FsmEstablishedTransitions	" The total number of times the BGP FSM transitioned into the established state for this peer." REFERENCE " RFC 4271, Section 8."

cbgpPeer2HoldTime	" Time interval (in seconds) for the Hold Timer established with the peer. The value of this object is calculated by this BGP speaker, using the smaller of the values in cbgpPeer2HoldTimeConfigured and the Hold Time received in the OPEN message. This value must be at least three seconds if it is not zero (0). If the Hold Timer has not been established with the peer this object MUST have a value of zero (0). If the cbgpPeer2HoldTimeConfigured object has a value of (0), then this object MUST have a value of (0)." REFERENCE " RFC 4271, Section 4.2."
cbgpPeer2HoldTimeConfigured	" Time interval (in seconds) for the Hold Time configured for this BGP speaker with this peer. This value is placed in an OPEN message sent to this peer by this BGP speaker, and is compared with the Hold Time field in an OPEN message received from the peer when determining the Hold Time (cbgpPeer2HoldTime) with the peer. This value must not be less than three seconds if it is not zero (0). If it is zero (0), the Hold Time is NOT to be established with the peer. The suggested value for this timer is 90 seconds." REFERENCE " RFC 4271, Section 4.2. RFC 4271, Section 10."
cbgpPeer2InTotalMessages	" The total number of messages received from the remote peer on this connection." REFERENCE " RFC 4271, Section 4."
cbgpPeer2InUpdateElapsedTime	" Elapsed time (in seconds) since the last BGP UPDATE message was received from the peer. Each time cbgpPeer2InUpdates is incremented, the value of this object is set to zero (0)." REFERENCE " RFC 4271, Section 4.3. RFC 4271, Section 8.2.2, Established state."
cbgpPeer2InUpdates	" The number of BGP UPDATE messages received on this connection." REFERENCE " RFC 4271, Section 4.3."
cbgpPeer2KeepAlive	" Time interval (in seconds) for the KeepAlive timer established with the peer. The value of this object is calculated by this BGP speaker such that, when compared with cbgpPeer2HoldTime, it has the same proportion that cbgpPeer2KeepAliveConfigured has, compared with cbgpPeer2HoldTimeConfigured. If the KeepAlive timer has not been established with the peer, this object MUST have a value of zero (0). If the of cbgpPeer2KeepAliveConfigured object has a value of (0), then this object MUST have a value of (0)." REFERENCE " RFC 4271, Section 4.4."

cbgpPeer2KeepAliveConfigured	" Time interval (in seconds) for the KeepAlive timer configured for this BGP speaker with this peer. The value of this object will only determine the KEEPALIVE messages' frequency relative to the value specified in cbgpPeer2HoldTimeConfigured; the actual time interval for the KEEPALIVE messages is indicated by cbgpPeer2KeepAlive. A reasonable maximum value for this timer would be one third of that of cbgpPeer2HoldTimeConfigured. If the value of this object is zero (0), no periodical KEEPALIVE messages are sent to the peer after the BGP connection has been established. The suggested value for this timer is 30 seconds." REFERENCE " RFC 4271, Section 4.4. RFC 4271, Section 10."
cbgpPeer2LastError	" The last error code and subcode seen by this peer on this connection. If no error has occurred, this field is zero. Otherwise, the first byte of this two byte OCTET STRING contains the error code, and the second byte contains the subcode." REFERENCE " RFC 4271, Section 4.5."
cbgpPeer2LastErrorTxt	" Implementation specific error description for bgpPeerLastErrorReceived."
cbgpPeer2LocalAddr	" The local IP address of this entry's BGP connection."
cbgpPeer2LocalAs	" The local AS number for this session."
cbgpPeer2LocalIdentifier	" The BGP Identifier of this entry's BGP peer."
cbgpPeer2LocalPort	" The local port for the TCP connection between the BGP peers."
cbgpPeer2MinASOriginationInterval	" Time interval (in seconds) for the MinASOriginationInterval timer. The suggested value for this timer is 15 seconds." REFERENCE " RFC 4271, Section 9.2.1.2. RFC 4271, Section 10."
cbgpPeer2MinRouteAdvertisementInterval	" Time interval (in seconds) for the MinRouteAdvertisementInterval timer. The suggested value for this timer is 30 seconds for EBGP connections and 5 seconds for IBGP connections." REFERENCE " RFC 4271, Section 9.2.1.1. RFC 4271, Section 10."
cbgpPeer2NegotiatedVersion	" The negotiated version of BGP running between the two peers. This entry MUST be zero (0) unless the cbgpPeer2State is in the openconfirm or the established state. Note that legal values for this object are between 0 and 255." REFERENCE " RFC 4271, Section 4.2. RFC 4271, Section 7."

cbgpPeer2OutTotalMessages	" The total number of messages transmitted to the remote peer on this connection." REFERENCE " RFC 4271, Section 4."
cbgpPeer2OutUpdates	" The number of BGP UPDATE messages transmitted on this connection." REFERENCE " RFC 4271, Section 4.3."
cbgpPeer2PrevState	" The BGP peer connection previous state." REFERENCE " RFC 1771, Section 8, A Border Gateway Protocol 4 (BGP-4)."
cbgpPeer2RemoteAs	" The remote autonomous system number received in the BGP OPEN message." REFERENCE " RFC 4271, Section 4.2."
cbgpPeer2RemoteIdentifier	" The BGP Identifier of this entry's BGP peer. This entry MUST be 0.0.0.0 unless the cbgpPeer2State is in the openconfirm or the established state." REFERENCE " RFC 4271, Section 4.2, 'BGP Identifier'."
cbgpPeer2RemotePort	" The remote port for the TCP connection between the BGP peers. Note that the objects cbgpPeer2LocalAddr, cbgpPeer2LocalPort, cbgpPeer2RemoteAddr, and cbgpPeer2RemotePort provide the appropriate reference to the standard MIB TCP conne.my
	ction table."
cbgpPeer2State	" The BGP peer connection state." REFERENCE " RFC 4271, Section 8.2.2."
cbgpPeerCapValue	" The value of the announced capability.REFERENCE " RFC 2842, Capabilities Advertisement with BGP-4. RFC2818, Route Refresh Capability for BGP-4. RFC2858, Multiprotocol Extensions for BGP-4. draft-ietf-idr-restart-05.txt, Graceful Restart Mechanism for BGP"
cbgpPeerLastErrorTxt	" Implementation specific error description for bgpPeerLastErrorReceived."

cbgpPeerPrefixAccepted	" Number of Route prefixes received on this connnection, which are accepted after applying filters. Possible filters are route maps, prefix lists, distributed lists, etc."
cbgpPeerPrefixAdvertised	" Counter which gets incremented when a route prefix is advertised on this connection. This object is initialized to zero when the peer is configured or the router is rebooted"
cbgpPeerPrefixDenied	" Counter which gets incremented when a route prefix received on this connection is denied or when a route prefix is denied during soft reset of this connection if 'soft-reconfiguration' is on . This object is initialized to zero when the peer is configured or the router is rebooted"
cbgpPeerPrefixLimit	" Max number of route prefixes accepted on this connection"
cbgpPeerPrefixSuppressed	" Counter which gets incremented when a route prefix is suppressed from being sent on this connection. This object is initialized to zero when the peer is configured or the router is rebooted"
cbgpPeerPrefixWithdrawn	" Counter which gets incremented when a route prefix is withdrawn on this connection. This object is initialized to zero when the peer is configured or the router is rebooted"
cbgpPeerPrevState	" The BGP peer connection previous state." REFERENCE " Section 8, RFC 1771, A Border Gateway Protocol 4 (BGP-4)."

CISCO-CLASS-BASED-QOS-MIB

This MIB provides read access to Quality of Service (QoS) configuration and statistics information for Cisco platforms that support the Modular Quality of Service Command-line Interface (Modular QoS CLI)

The following table lists the tables associated with this MIB:

MIB Name	Description
cbQosAtmVCI	" VCI for the ATMVC to which this service is attached. This field only make sense if the service policy is attached to a ATM VC."
cbQosAtmVPI	" VPI for the ATMVC to which this service is attached. This field only make sense if the service policy is attached to a ATM VC."
cbQosCMDesc	" Description of the Classmap."
cbQosCMDropBitRate	" The bit rate of the drops per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."

cbQosCMDropBitRate64	" The bit rate of the drops per class as the result of all features that can produce drops (e.g., police, random detect, etc.). This object is a 64-bit version of cbQosCMDropBitRate."
cbQosCMDropByte	" The lower 32 bits counter of dropped bytes per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMDropByte64	" The 64 bits counter of dropped bytes per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMDropByteOverflow	" The upper 32 bits counter of dropped bytes per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMDropPkt	" The lower 32 bits counter of dropped pkts per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMDropPkt64	" The 64 bits counter of dropped pkts per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMDropPktOverflow	" The upper 32 bits counter of dropped pkts per class as the result of all features that can produce drops (e.g., police, random detect, etc.)."
cbQosCMInfo	" Match all vs Match any in a given class."
cbQosCMName	" Name of the Classmap."
cbQosCMPostPolicyBitRate	" The bit rate of the traffic after executing QoS policies."
cbQosCMPostPolicyBitRate64	" The bit rate of the traffic after executing QoS policies. This object is a 64-bit version of cbQosCMPostPolicyBitRate."
cbQosCMPostPolicyByte	" The lower 32 bits count of outbound octets after executing QoS policies."
cbQosCMPostPolicyByte64	" The 64 bits count of outbound octets after executing QoS policies."
cbQosCMPostPolicyByteOverflow	" The upper 32 bits count of outbound octets after executing QoS policies."
cbQosCMPrePolicyBitRate	" The bit rate of the traffic prior to executing any QoS policies."
cbQosCMPrePolicyBitRate64	" The bit rate of the traffic prior to executing any QoS policies.This object is a 64-bit version of cbQosCMPrePolicyBitRate."
cbQosCMPrePolicyByte	" The lower 32 bits count of inbound octets prior to executing any QoS policies."
cbQosCMPrePolicyByte64	" The 64 bits count of inbound octets prior to executing any QoS policies."
cbQosCMPrePolicyByteOverflow	" The upper 32 bits count of inbound octets prior to executing any QoS policies."

cbQosCMPrePolicyPkt	" The lower 32 bits count of inbound packets prior to executing any QoS policies."
cbQosCMPrePolicyPkt64	" The 64 bits count of inbound packets prior to executing any QoS policies."
cbQosCMPrePolicyPktOverflow	" The upper 32 bits count of inbound packets prior to executing any QoS policies."
cbQosConfigIndex	" An arbitrary (system-assigned) config (instance independent) index for each Object. Each objects having the same configuration share the same config index."
cbQosEntityIndex	" In cases where the policy is attached to an entity e.g. control-plane, this object represents the entity physical index of the entity to which the policy has been attached. A value zero may be returned if the policy is not attached to a physical entity or the entPhysicalTable is not supported on the SNMP agent."
cbQosFrDLCI	" DLCI for the FRVC to which this service is attached. This field only make sense if the service policy is attached to a Frame Relay DLCI."
cbQosIfIndex	" ifIndex for the interface to which this service is attached. This field makes sense only if the logical interface has a snmp ifIndex. For e.g. the value of this field is meaningless when the cbQosIfType is controlPlane."
cbQosIFPolicyIndex	" An arbitrary (system-assigned) index for all Service Policies. This is identical to cbQosPolicyIndex."
cbQosIfType	" This describes the logical interface/media type to which this service policy is attached."
cbQosMatchStmtInfo	" Match vs Match Not in a given class."
cbQosMatchStmtName	" Name of the Match Statement."
cbQosObjectsType	" The type of the QoS object."
cbQosParentObjectsIndex	" The parent instance index of a QoS object. For a ClassMap, the parent index would be the index of the attached PolicyMap. For a Match Statement, the parent index would be the index of the ClassMap that uses this Match Statement. For an action, the parent index would be the index of the ClassMap that applies such Action. For a non-hierarchical PolicyMap, the parent would be the logical interface to which the policy is attached, thus the parent index would be 0. For a hierarchical PolicyMap, the parent index would be the index of the ClassMap to which the nested policy is attached."

cbQosParentPolicyIndex	" The value refering to service-policy index of a virtual interface on which PolicyMap applied directly. Value set would imply the entry is for a physical interface which is a member of a virtual interface. Value zero implies the entry is for a interface on which PolicyMap applied directly."
cbQosPoliceCfgBurstSize	" The amount of traffic, in bytes, in excess of the committed policing rate that will be permitted by the policing feature. cbQosPoliceCfgBurstSize object is superseded by cbQosPoliceCfgBurstSize64."
cbQosPoliceCfgBurstSize64	" This object indicated the amount of traffic, in bytes, in excess of the committed policing rate that will be permitted by the policing feature. If a device implements cbQosPoliceCfgBurstSize64, then it should not implement cbQosPoliceCfgBurstSize."
cbQosPoliceCfgCdvt	" The ATM Cell Delay Variation Tolerance value."
cbQosPoliceCfgConditional	" This object is use to depict weather police is configured as a conditioniler policer or not"
cbQosPoliceCfgConformColor	" The Classmap name used in AF color-aware mode to specify the conform-color for the incoming packets which was marked by the previous node. At least conform-color must be specified. If only conform-color is specified, all other packets are assumed to be marked exceed. See RFC 2697, A Single Rate Three Color Marker. See RFC 2698, A Two Rate Three Color Marker."
cbQosPoliceCfgExceedColor	" The Classmap name used in AF color-aware mode to specify the exceed-color for the incoming packets which was marked by the previous node. If both conform-color and exceed-color are specified, all other packets are assumed to be marked violate. Violate-color configuration is not needed."
cbQosPoliceCfgPercentRateValue	" The committed policing rate in percentage. Its value is valid only when cbQosPoliceCfgRateType equals to 2."
cbQosPoliceCfgPir	" The committed policing rate. This is the peak rate permitted by two rate policing. cbQosPoliceCfgPir object is superseded by cbQosPoliceCfgPir64."
cbQosPoliceCfgPir64	" This object indicates the committed policing rate. This is the peak rate permitted by two rate policing. If a device implements cbQosPoliceCfgPir64, then it should not implement cbQosPoliceCfgPir."
cbQosPoliceCfgRate	" The committed policing rate. This is the sustained rate permitted by policing. If a committed policing rate greater than 4294967295 is configurable on the system, then the configured rate is available in cbQosPoliceCfgRate64."

cbQosPoliceCfgRate64	" The committed policing rate. This is the sustained rate permitted by policing."
cbQosPoliceCfgRateType	" The rate type that configured for CIR & PIR. 1 means rates are configured in bps. 2 means rates are configured in percentage. 3 means rates are configured in cps. 4 means rates are configured in parts per-thousand. 5 means rates are configured in parts per-million."
cbQosPoliceCfmColorCfmBitRate	" The bit rate of conform color class conform rate."
cbQosPoliceCfmColorCfmByte64	" The 64 bits count of bytes which are marked as Conform-Color by previous node and treated as conforming by the policing feature on this node."
cbQosPoliceCfmColorCfmPkt64	" The 64 bits count of packets which are marked as Conform-Color by previous node and treated as conforming by the policing feature on this node."
cbQosPoliceCfmColorExdBitRate	" The bit rate of conform color class exceed rate."
cbQosPoliceCfmColorExdByte64	" The 64 bits count of bytes which are marked as Conform-Color by previous node and treated as exceeding by the policing feature on this node."
cbQosPoliceCfmColorExdPkt64	" The 64 bits count of packets which are marked as Conform-Color by previous node and treated as exceeding by the policing feature on this node."
cbQosPoliceCfmColorVltBitRate	" The bit rate of conform color class violate rate."
cbQosPoliceCfmColorVltByte64	" The 64 bits count of bytes which are marked as Conform-Color by previous node and treated as violating by the policing feature on this node."
cbQosPoliceCfmColorVltPkt64	" The 64 bits count of packets which are marked as Conform-Color by previous node and treated as violating by the policing feature on this node."
cbQosPoliceConformedBitRate	" The bit rate of conforming traffic."
cbQosPoliceConformedBitRate64	" The bit rate of conforming traffic. This object is a 64-bit version of cbQosPoliceConformedBitRate."
cbQosPoliceConformedByte	" The lower 32 bits count of octets treated as conforming by the policing feature."
cbQosPoliceConformedByte64	" The 64 bits count of octets treated as conforming by the policing feature."
cbQosPoliceConformedByteOverflow	" The upper 32 bits count of octets treated as conforming by the policing feature."
cbQosPoliceConformedPkt	" The lower 32 bits count of packets treated as conforming by the policing feature."
cbQosPoliceConformedPkt64	" The 64 bits count of packets treated as conforming by the policing feature."

cbQosPoliceConformedPktOverflow	"The upper 32 bits count of packets treated as conforming by the policing feature."
cbQosPoliceExceededBitRate	"The bit rate of the non-conforming traffic."
cbQosPoliceExceededBitRate64	"The bit rate of non-conforming traffic. This object is a 64-bit version of cbQosPoliceExceededBitRate."
cbQosPoliceExceededByte	"The lower 32 bits count of octets treated as non-conforming by the policing feature."
cbQosPoliceExceededByte64	"The 64 bits count of octets treated as non-conforming by the policing feature."
cbQosPoliceExceededByteOverflow	"The upper 32 bits count of octets treated as non-conforming by the policing feature."
cbQosPoliceExceededPkt	"The 32 bits count of packets treated as non-conforming by the policing feature."
cbQosPoliceExceededPkt64	"The 64 bits count of packets treated as non-conforming by the policing feature."
cbQosPoliceExceededPktOverflow	"The upper 32 bits count of packets treated as non-conforming by the policing feature."
cbQosPoliceExdColorExdBitRate	"The bit rate of exceed color class exceed rate."
cbQosPoliceExdColorExdByte64	"The 64 bits count of bytes which are marked as Exceed-Color by previous node and treated as exceeding by the policing feature on this node."
cbQosPoliceExdColorExdPkt64	"The 64 bits count of packets which are marked as Exceed-Color by previous node and treated as exceeding by the policing feature on this node."
cbQosPoliceExdColorVltBitRate	"The bit rate of exceed color class violate rate."
cbQosPoliceExdColorVltByte64	"The 64 bits count of bytes which are marked as Exceed-Color by previous node and treated as violating by the policing feature on this node."
cbQosPoliceExdColorVltPkt64	"The 64 bits count of packets which are marked as Exceed-Color by previous node and treated as violating by the policing feature on this node."
cbQosPoliceViolatedBitRate	"The bit rate of the violating traffic."
cbQosPoliceViolatedBitRate64	"The bit rate of the violating traffic. This object is a 64-bit version of cbQosPoliceViolatedBitRate."
cbQosPoliceViolatedByte	"The lower 32 bits count of octets treated as violated by the policing feature."
cbQosPoliceViolatedByte64	"The 64 bits count of octets treated as violated by the policing feature."
cbQosPoliceViolatedByteOverflow	"The upper 32 bits count of octets treated as violated by the policing feature."
cbQosPoliceViolatedPkt	"The 32 bits count of packets treated as violated by the policing feature."
cbQosPoliceViolatedPkt64	"The 64 bits count of packets treated as violated by the policing feature."

cbQosPoliceViolatedPktOverflow	" The upper 32 bits count of packets treated as violated by the policing feature."
cbQosPoliceVltColorVltBitRate	" The bit rate of violate color class violate rate."
cbQosPoliceVltColorVltByte64	" The 64 bits count of bytes which are marked as Violate-Color by previous node and treated as violating by the policing feature on this node."
cbQosPoliceVltColorVltPkt64	" The 64 bits count of packets which are marked as Violate-Color by previous node and treated as violating by the policing feature on this node."
cbQosPolicyDirection	" This indicates the direction of traffic for which this service policy is applied."
cbQosPolicyDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more objects of cbQosServicePolicyEntry table for a given instance suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, this object contains a zero value."
cbQosPolicyMapDesc	" Description of the PolicyMap."
cbQosPolicyMapName	" Name of the Policymap."
cbQosQueueingCfgAggregateQLimit	" Maximum allowed queue size for all the individual queues associated with this class. When the queue size exceed this value, the packets will be dropped."
cbQosQueueingCfgAggrQLimitTime	" Maximum allowed queue size in milli-seconds for all individual queues associated with this class. It is internally converted to bytes by using the bandwidth that is available for the class."

cbQosQueueingCfgBandwidth	" The type of bandwidth configuration value represented by this object is indicated by the value of cbQosQueueingCfgBandwidthUnits for this entry. If the cbQosQueueingCfgBandwidthUnits value is 'kbps(1)' or 'percentage(2)', this object represents the configured bandwidth allocated to this traffic class.In the case of a bandwidth policy, this value represents a minimum bandwidth guarantee for the traffic class. In the case of a priority policy, this value represents the maximum rate at which priority service is guaranteed. If the cbQosQueueingCfgBandwidthUnits value is 'percentageRemaining(3)', this object represents the the percentage of the unallocated bandwidth to allocate to this class. If the cbQosQueueingCfgBandwidthUnits value is 'ratioRemaining(4)', this object represents the ratio value, relative to other class' configured ratio values, used to determine the portion of the unallocated bandwidth to apply to this class. cbQosQueueingCfgBandwidth object is superseded by cbQosQueueingCfgBandwidth64."
cbQosQueueingCfgBandwidthUnits	" Units of the accompanying cbQosQueueingCfgbandwidth parameter"
cbQosQueueingCfgIndividualQSize	" Maximum number of packets that can be held in an individual Flow-based fair-queue associated with this class before it drops packets (once the AggregateQSize has been reached). This field only makes sense in the context of Flow-based fair-queueing. cbQosQueueingCfgIndividualQSize object is superseded by cbQosQueueingCfgIndividualQSize64."
cbQosQueueingCfgIndividualQSize64	" Maximum number of packets that can be held in an individual Flow-based fair-queue associated with this class before it drops packets (once the AggregateQSize has been reached). If a device implements cbQosQueueingCfgIndividualQSize64, then it should not implement cbQosQueueingCfgIndividualQSize."
cbQosQueueingCfgPriorityEnabled	" Boolean to indicate if low latency queueing (priority) is enabled for this class."
cbQosQueueingCfgPriorityLevel	" The priority level of the queue into which packets matching this class are queued into. A larger priority level indicates higher priority."
cbQosQueueingCfgQLimitUnits	" Represents the unit type of cbQosQueueingCfgAggregateQLimit object."
cbQosQueueingCurrentQDepth	" The current depth of the queue."
cbQosQueueingCurrentQDepthPkt	" The current number of packets sitting in the queue"

cbQosQueueingDiscardByte	" The lower 32 bits count of octets, associated with this class, that were dropped by queueing."
cbQosQueueingDiscardByte64	" The count of octets, associated with this class, that were dropped by queueing."
cbQosQueueingDiscardByteOverflow	" The upper 32 bit count of octets, associated with this class, that were dropped by queueing."
cbQosQueueingDiscardPkt	" The number of packets, associated with this class, that were dropped by queueing."
cbQosQueueingDiscardPkt64	" The number of packets, associated with this class, that were dropped by queueing."
cbQosQueueingDiscardPktOverflow	" The upper 32 bits count of packets, associated with this class, that were dropped by queueing."
cbQosQueueingMaxQDepth	" The maximum depth of the queue."
cbQosQueueingMaxQDepthPkt	" The maximum depth of the queue in packets."
cbQosQueueingTransmitByte64	" The count of octets, associated with this class, that were transmitted by queueing."
cbQosQueueingTransmitPkt64	" The number of packets, associated with this class, that were transmitted by queueing."
cbQosREDCfgDscpPrec	" The Classification mechanism used by RED"
cbQosREDCfgPktDropProb	" Denominator for the fraction of packets dropped when the average queue depth is MaxDepthThreshold. For example, if the denominator is 10, one out of every 10 packets is dropped when the average queue is at the MaxDepthThreshold."
cbQosREDClassCfgMaxThreshold	" The maximum WRED threshold value. When the average queue length exceeds this number, WRED drops all packets according to REDMechanism specificed in cbQosREDCfgDscpPrec."
cbQosREDClassCfgMaxThresholdTime	" The maximum WRED threshold value specified in milli-seconds. The milli-second value is internally converted to bytes by using the bandwidth that is available for the class."
cbQosREDClassCfgMaxThresholdUnit	" Represents the unit type to measure the RED Maximum thresholds. The objects covered is cbQosREDClassCfgMaxThreshold"
cbQosREDClassCfgMinThreshold	" The minimum WRED threshold value. When the average queue length reaches this number, WRED begins to drop packets according to REDMechanism specificed in cbQosREDCfgDscpPrec."
cbQosREDClassCfgMinThresholdTime	" The minimum WRED threshold value specified in milli-seconds. The milli-second value is internally converted to bytes by using the bandwidth that is available for the class."
cbQosREDClassCfgMinThresholdUnit	" Represents the unit type to measure the RED Minimum thresholds. The objects covered is cbQosREDClassCfgMinThreshold"

cbQosSetCfgDiscardClassValue	" The Discard Class value at which the packet is being set by the packet marking feature."
cbQosSetCfgFeature	" The bit-wise position of each packet marking feature."
cbQosSetCfgL2CosValue	" The Layer 2 Cos value at which the packet is being set by the packet marking feature."
cbQosSetCfgMplsExpValue	" The MPLS experimental value at which the packet is being set by the packet marking feature."
cbQosSetCfgQosGroupValue	" The QoS Group number at which the packet is being set by the packet marking feature."
cbQosTSCfgBurstTime	" The amount of traffic, in ms, in excess of the committed traffic-shaping rate that will be instantaneously permitted by this feature. The milli-second value is internally converted to bits by using the bandwidth that is available for the class."
cbQosTSCfgExtBurstSize	" The amount of traffic, in bits, in excess of the burst limit, which may be conditionally permitted by traffic-shaping feature. cbQosTSCfgExtBurstSize object is superseded by cbQosTSCfgExtBurstSize64."
cbQosTSCfgExtBurstSize64	" This object indicates the amount of traffic, in bits, in excess of the burst limit, which may be conditionally permitted by traffic-shaping feature. If a device implements cbQosTSCfgExtBurstSize64, then it should not implement cbQosTSCfgExtBurstSize."
cbQosTSCfgExtBurstTime	" The amount of traffic, in ms, in excess of the burst limit, which may be conditionnally permitted by traffic-shaping feature. The milli-second value is internally converted to bits by using the bandwidth that is available for the class."
cbQosTSCfgLimitType	" This object indicates if traffic-shaping is limiting traffic based on the peak rate or the average rate."
cbQosTSCfgPercentRateValue	" The committed traffic-shaping rate in percentage. Its value is valid only when cbQosTSCfgRateType equals to 2."
cbQosTSCfgRate	" The committed traffic-shaping rate. This is the sustained rate permitted by the traffic-shaping."
cbQosTSCfgRate64	" The committed shape rate. This is the sustained rate permitted by shaping. This object represents the 64 bit value of object cbQosTSCfgRate"
cbQosTSCfgRateType	" The rate type that configured for traffic-shaping. 1 means rate is configured in bps. 2 means rate is configured in percentage. 4 means rates are configured in parts per-thousand. 5 means rates are configured in parts per-million."
cbQosTSStatsDropByte	" This object represents the lower 32 bits counter of octets that have been dropped during shaping."
cbQosTSStatsDropByte64	" This object represents the 64 bits counter of octets that have been dropped during shaping."

cbQosTSStatsDropByteOverflow	" This object represents the upper 32 bits counter of octets that have been dropped during shaping."
cbQosTSStatsDropPkt	" This object represents the lower 32 bits counter of packets that have been dropped during shaping."
cbQosTSStatsDropPkt64	" This object represents the 64 bits counter of packets that have been dropped during shaping."
cbQosTSStatsDropPktOverflow	" This object represents the upper 32 bits counter of packets that have been dropped during shaping."
cbQosVlanIndex	" If the service policy is attached to a particular vlan on a trunk or multi-vlan access port, then this object specifies the corresponding VLAN. In all other cases the value of this object is '0'."

CISCO-CONFIG-MAN-MIB

Configuration management MIB The MIB represents a model of configuration data that exists in various locations

running in use by the running system

terminal saved to whatever is attached as the terminal

local saved locally in NVRAM or flash

remote saved to some server on the network

The following table lists the tables associated with this MIB:

MIB Name	Description
ccmHistoryEventCommandSource	" The source of the command that instigated the event."
ccmHistoryEventCommandSourceAddress	" If ccmHistoryEventTerminalType is 'virtual', the internet address of the connected system. If ccmHistoryEventCommandSource is 'snmp', the internet address of the requester. The value is 0.0.0.0 if not available or not applicable. This object is deprecated by ccmHistoryEventCommandSourceAddrRev1"
ccmHistoryEventConfigDestination	" The configuration data destination for the event."
ccmHistoryEventConfigSource	" The configuration data source for the event."
ccmHistoryEventEntriesBumped	" The number of times the oldest entry in ccmHistoryEventTable was deleted to make room for a new entry."

ccmHistoryEventFile	" If ccmHistoryEventConfigSource or ccmHistoryEventConfigDestination is 'networkTftp' or 'networkRcp', the configuration file name at the storage file server. The length is zero if not available or not applicable."
ccmHistoryEventRcpUser	" If ccmHistoryEventConfigSource or ccmHistoryEventConfigDestination is 'networkRcp', the remote user name. The length is zero if not applicable or not available."
ccmHistoryEventServerAddress	" If ccmHistoryEventConfigSource or ccmHistoryEventConfigDestination is 'networkTftp' or 'networkRcp', the internet address of the storage file server. The value is 0.0.0.0 if not applicable or not available. This object is deprecated by ccmHistoryEventServerAddrRev1"
ccmHistoryEventTerminalLocation	" If ccmHistoryEventCommandSource is 'commandLine', the hard-wired location of the terminal or the remote host for an incoming connection. The length is zero if not available or not applicable."
ccmHistoryEventTerminalNumber	" If ccmHistoryEventCommandSource is 'commandLine', the terminal number. The value is -1 if not available or not applicable."
ccmHistoryEventTerminalType	" If ccmHistoryEventCommandSource is 'commandLine', the terminal type, otherwise 'notApplicable'."
ccmHistoryEventTerminalUser	" If ccmHistoryEventCommandSource is 'commandLine', the name of the logged in user. The length is zero if not available or not applicable."
ccmHistoryEventTime	" The value of sysUpTime when the event occurred."
ccmHistoryEventVirtualHostName	" If ccmHistoryEventTerminalType is 'virtual', the host name of the connected system. The length is zero if not available or not applicable."
ccmHistoryMaxEventEntries	" The maximum number of entries that can be held in ccmHistoryEventTable. The recommended value for implementations is 10."
ccmHistoryRunningLastChanged	" The value of sysUpTime when the running configuration was last changed. If the value of ccmHistoryRunningLastChanged is greater than ccmHistoryRunningLastSaved, the configuration has been changed but not saved."

ccmHistoryRunningLastSaved	" The value of sysUpTime when the running configuration was last saved (written). If the value of ccmHistoryRunningLastChanged is greater than ccmHistoryRunningLastSaved, the configuration has been changed but not saved. What constitutes a safe saving of the running configuration is a management policy issue beyond the scope of this MIB. For some installations, writing the running configuration to a terminal may be a way of capturing and saving it. Others may use local or remote storage. Thus ANY write is considered saving for the purposes of the MIB."
ccmHistoryStartupLastChanged	" The value of sysUpTime when the startup configuration was last written to. In general this is the default configuration used when cold starting the system. It may have been changed by a save of the running configuration or by a copy from elsewhere."
CISCO-CDP-MIB	" The MIB module for management of the Cisco Discovery Protocol in Cisco devices."
cdpGlobalDeviceId	" The device ID advertised by this device. The format of this device id is characterized by the value of cdpGlobalDeviceIdFormat object."
cdpGlobalHoldTime	" The time for the receiving device holds CDP message. The default value is 180 seconds."
cdpGlobalMessageInterval	" The interval at which CDP messages are to be generated. The default value is 60 seconds."
cdpGlobalRun	" An indication of whether the Cisco Discovery Protocol is currently running. Entries in cdpCacheTable are deleted when CDP is disabled."
CISCO-ENTITY-ASSET-MIB	" Monitor the asset information of items in the ENTITY-MIB (RFC 2037) entPhysical table."
ceAssetCLEI	" This object represents the CLEI (Common Language Equipment Identifier) code for the physical entity. If the physical entity is not present in the system, or does not have an associated CLEI code, then the value of this object will be a zero-length string." REFERENCE " Bellcore Technical reference GR-485-CORE, COMMON LANGUAGE Equipment Processes and Guidelines, Issue 2, October, 1995."
ceAssetEntry	" An entAssetEntry entry describes the asset-tracking related data for an entity." INDEX { entPhysicalIndex }

ceAssetFirmwareID	" This variable indicates the firmware installed on this entity. For IOS devices, this variable's value is in the IOS Image Naming Convention format. IOS Image Naming Convention Software images are named according to a scheme that identifies what's in the image and what platform it runs on. The names have three parts, separated by dashes: e.g. xxxx-yyyy-ww. xxxx = Platform yyyy = Features ww = Where it executes from and if compressed "
ceAssetMfgAssyNumber	" This variable indicates the manufacturing assembly number, which is the 'hardware' identification."
ceAssetMfgAssyRevision	" This variable indicates the revision of the entity, within the ceAssetMfgAssyNumber."
ceAssetSoftwareID	" This variable indicates the software installed on this entity. For IOS devices, this variable's value is in the IOS Image Naming Convention format. IOS Image Naming Convention Software images are named according to a scheme that identifies what's in the image and what platform it runs on. The names have three parts, separated by dashes: e.g. xxxx-yyyy-ww. xxxx = Platform yyyy = Features ww = Where it executes from and if compressed "

CISCO-ENTITY-ASSET-MIB

Monitor the asset information of items in the ENTITY-MIB (RFC 2037) entPhysical table.

The following table lists the tables associated with this MIB:

MIB Name	Description
ceExtEntBreakOutPortNotifEnable	" This object controls the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved as follows: 'true(1)' - the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved notifications is enabled. 'false(2)' - the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved notifications is disabled."
ceExtEntDoorNotifEnable	" This object controls the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications as follows: 'true(1)' - the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications are enabled. 'false(2)' - the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications are disabled."

CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB is used to monitor and configure operational status of Field Replaceable Units (FRUs) and other manageable physical entities of the system listed in the Entity-MIB (RFC 2737) entPhysicalTable.

The following table lists the tables associated with this MIB:

MIB Name	Description
cefcFanTrayOperStatus	" The operational state of the fan or fan tray. unknown(1) - unknown. up(2) - powered on. down(3) - powered down. warning(4) - partial failure, needs replacement as soon as possible."
cefcFRUCurrent	" Current supplied by the FRU (positive values) or current required to operate the FRU (negative values)."
cefcFRUPowerAdminStatus	" Administratively desired FRU power state."
cefcFRUPowerOperStatus	" Operational FRU power state."
cefcMIBEnableStatusNotification	" This variable indicates whether the system produces the following notifications: cefcModuleStatusChange, cefcPowerStatusChange, cefcFRUInserted, cefcFRURemoved, cefcUnrecognizedFRU and cefcFanTrayStatusChange. A false value will prevent these notifications from being generated."
cefcModuleAdminStatus	" This object provides administrative control of the module."
cefcModuleLastClearConfigTime	" The value of sysUpTime when the configuration was most recently cleared."
cefcModuleOperStatus	" This object shows the module's operational state."
cefcModuleResetReason	" This object identifies the reason for the last reset performed on the module."
cefcModuleStatusLastChangeTime	" The value of sysUpTime at the time the cefcModuleOperStatus is changed."
cefcModuleUpTime	" This object provides the up time for the module since it was last re-initialized. This object is not persistent; if a module reset, restart, power off, the up time starts from zero."
cefcPhysicalStatus	" The status of this physical entity. other(1) - the status is not any of the listed below. supported(2) - this entity is supported. unsupported(3) - this entity is unsupported. incompatible(4) - this entity is incompatible. It would be unsupported(3), if the ID read from Serial EPROM is not supported. It would be incompatible(4), if in the present configuration this FRU is not supported."

CISCO-ENHANCED-MEMPOOL-MIB

New MIB module for monitoring the memory pools of all physical entities on a managed system

The following table lists the tables associated with this MIB:

MIB Name	Description
cempMemPoolAlternate	" Indicates whether or not this memory pool has an alternate pool configured. Alternate pools are used for fallback when the current pool runs out of memory. If an instance of this object has a value of zero, then this pool does not have an alternate. Otherwise the value of this object is the same as the value of cempMemPoolType of the alternate pool."
cempMemPoolFree	" Indicates the number of bytes from the memory pool that are currently unused on the physical entity. Note that the sum of cempMemPoolUsed and cempMemPoolFree is the total amount of memory in the pool"
cempMemPoolFreeOvrflw	" This object represents the upper 32-bits of cempMemPoolFree. This object needs to be supported only if the unused bytes in the memory pool exceeds 32-bits, otherwise this object value would be set to 0."
cempMemPoolHCFree	" Indicates the number of bytes from the memory pool that are currently unused on the physical entity. This object is a 64-bit version of cempMemPoolFree."
cempMemPoolHCUsed	" Indicates the number of bytes from the memory pool that are currently in use by applications on the physical entity. This object is a 64-bit version of cempMemPoolUsed."
cempMemPoolName	" A textual name assigned to the memory pool. This object is suitable for output to a human operator, and may also be used to distinguish among the various pool types."
cempMemPoolType	" The type of memory pool for which this entry contains information."
cempMemPoolUsed	" Indicates the number of bytes from the memory pool that are currently in use by applications on the physical entity."
cempMemPoolUsedOvrflw	" This object represents the upper 32-bits of cempMemPoolUsed. This object needs to be supported only if the used bytes in the memory pool exceeds 32-bits, otherwise this object value would be set to 0."

cempMemPoolValid	" Indicates whether or not cempMemPoolUsed, cempMemPoolFree, cempMemPoolLargestFree and cempMemPoolLowestFree in this entry contain accurate data. If an instance of this object has the value false (which in and of itself indicates an internal error condition), the values of these objects in the conceptual row may contain inaccurate information (specifically, the reported values may be less than the actual values)."

CISCO-ENTITY-REDUNDANCY-MIB

This management information module supports configuration, control and monitoring of redundancy protection for various kinds of components on Cisco managed devices.

The following table lists the tables associated with this MIB:

MIB Name	Description
ceRedunEnableStatusChangeNotifs	" This object controls whether the system produces ceRedunProtectStatusChange notifications. A false value will prevent ceRedunProtectStatusChange notifications from being generated by this system. "
ceRedunEnableSwitchoverNotifs	" This object controls whether the system produces ceRedunEventSwitchover notifications. A false value will prevent ceRedunEventSwitchover notifications from being generated by this system. "
ceRedunGroupArch	" The architecture of the redundancy group, such as 1:1 or 1:n, etc. This object may not be modified if the associated ceRedunGroupRowStatus object is equal to active(1). "
ceRedunGroupCounts	" The current count of redundancy groups for a specific ceRedunGroupTypeIndex. This count indicates the number of rows in the ceRedunGroupTable for a specific ceRedunGroupTypeIndex. "

ceRedunGroupDefinitionChanged	" The value of sysUpTime when there was the most recent change to any objects in the ceRedunGroupTypesTable except for ceRedunGroupCounts or ceRedunNextUnusedGroupIndex. The sysUpTime should also reflect changes to either the ceRedunVendorTypesTable, ceRedunInternalStatesTable or ceRedunSwitchoverReasonTable. Normally these objects are static, but if there was an in service upgrade to the software image of the managed system then the tables may change and should be read again. If there has been no change since the last initialization of the local network management system, this object should contain the value 0. "
ceRedunGroupLastChanged	" The value of sysUpTime corresponding to the last change for any object in the ceRedunGroupTable. The source of the change can be due to either an SNMP message affecting an object in the table or due to any other source of user input such as a command line interface. The timestamp applies to all read-create objects even for cases where the managed device only supports read-only access because it doesn't require user configuration of those objects. If there has been no change since the last time the sysUpTime was zero then report the sysUpTime as zero. "
ceRedunGroupRedunType	" The intended type of redundancy protection such as 'yCable' or 'aps' for this redundancy group. "
ceRedunGroupRevert	" The revertive mode of the redundancy group. nonrevertive(1) The secondary member remains active until another switchable event takes place. revertive(2) When the condition that caused a switch to the secondary member has been cleared, a switch is made back to the primary member after a configured delay. Switching should normally be revertive for the 1:n and load-sharing architectures. Switching may optionally be revertive with the 1:1 and 1+1 architectures. This object may not be modified if the associated ceRedunGroupRowStatus object is equal to active(1). "

ceRedunGroupRowStatus	" The configuration status of this redundancy group entry. An entry may not exist in the active RowStatus state unless all configurable read-create objects in the entry have an appropriate value. No other read-create objects in this group may be modified if the ceRedunGroupRowStatus object is equal to active(1). When set to 'notInService', changes may be made to configurable read-create objects. Also, associated ceRedunMbrTable objects may be added, deleted and modified. After modifying a conceptual row in this table, the management client must set this object to 'active' in order for the changes to take effect. "
ceRedunGroupScope	" This object determines the local/remote scope of the redundancy group. This object may not be modified if the associated ceRedunGroupRowStatus object is equal to active(1). "
ceRedunGroupStorageType	" The storage type for this conceptual row. By default, the row will not be saved into non-volatile memory unless this object is set to the value nonVolatile. Note: Conceptual rows having the value 'readOnly' can be used for redundancy groups that aren't configurable and need not allow write-access to any columnar objects in the row. "
ceRedunGroupString	" If ceRedunUsesGroupName is 'true' for this redundancy group type, this object is a group name identifier and the value of this object has to be specified and should contain no internal spaces when configuring this group entry. If ceRedunUsesGroupName is 'false', the ceRedunGroupString object is just used as an optional description for the group rather than as the group name. In that case it's allowed to have spaces in the string. "
ceRedunGroupTypeName	" The textual name of the redundancy group type. The value of this object should be the name of the redundancy group type assigned by the local device as it would appear for display commands entered at the device's `console'. Examples are port-group, linecard-group, fan-group, etc. "
ceRedunInternalStateDescr	" This is a string description for the specific internal member state. "
ceRedunMaxMbrsInGroup	" The maximum number of primary plus secondary members allowed in a group for a specific ceRedunGroupTypeIndex. If only 1:1 or 1+1 is supported, this should be 2. If the maximum number is unknown or not determinable, the managed system should return 0. "

ceRedunMbrInternalState	" This is the current internal state index for a member. The corresponding state category and description can be found in the ceRedunInternalStatesTable. It may include any of the initialization or intermediate progression states necessary to reach a stable active or standby state. "
ceRedunMbrLastChanged	" The value of sysUpTime corresponding to the last change to any read-create objects in this table. The source of the change can be due to either an SNMP message affecting this table or due to any other source of user input such as a command line interface. The timestamp applies to all read-create objects even for cases where the managed device only supports read-only access because it doesn't require user configuration of those objects. If there has been no change since the last time the sysUpTime was zero then report the sysUpTime as zero. "
ceRedunMbrLastSwitchover	" The value of sysUpTime when this primary member last completed a switchover to the secondary member. If this member has never switched to standby, or this is a secondary member, the value 0 should be returned. "
ceRedunMbrMode	" This field is set to the 'primary' (working) or 'secondary' (protection) role within the redundancy group. The designation as 'primary' or 'secondary' is configured and is static. It doesn't change due to a switchover. "
ceRedunMbrPhysIndex	" This field specifies the entity PhysicalIndex which is being configured as a redundancy member. It is the responsibility of the managed device to enforce any restrictions on matching entPhysicalVendorType, slot positions etc. among members of the same redundancy group. "
ceRedunMbrProtectingMbr	" This field is valid only for a secondary member. When the secondary member is active, this value indicates the primary member it has taken over for. When the secondary member is standby, it should return its own member number. Primary members should return their own member number. "
ceRedunMbrRowStatus	" The configuration status of this member entry. A row in the ceRedunMbrConfigTable may not be created, deleted, or set to notInService if the associated ceRedunGroupRowStatus object is equal to active. However, if the ceRedunGroupRowStatus object is equal to notInService, a row may be created, deleted or modified. In other words, a member may not be added, deleted or modified if the including group is active. "
ceRedunMbrStatusCurrent	" Indicates the current status bitflags for the member. "

ceRedunMbrStatusLastChanged	" The value of sysUpTime corresponding to the last change to any objects in the ceRedunMbrStatusTable table. If there has been no change since the last time the sysUpTime was zero then report the sysUpTime as zero. "
ceRedunMbrStorageType	" The storage type for this conceptual row. By default, the row will not be saved into non-volatile memory unless this object is set to the value nonVolatile. Note: Conceptual rows having the value 'readOnly' can be used for redundancy groups that aren't configurable and need not allow write-access to any columnar objects in the row. "
ceRedunMbrSwitchoverCounts	" The number of times this primary or secondary member has changed from being active to being standby due to a switchover. The counter should monotonically increase but never wrap or decrease, except at a system restart. When queried for a secondary member that has never gone active since the last system restart, then no switchovers should be reported so it should return 0. "
ceRedunMbrSwitchoverReason	" The reported reason code for the last switchover. The corresponding reason category and description can be found from the ceRedunSwitchoverReasonTable. "
ceRedunNextUnusedGroupIndex	" The next unused group index available for configuring a new redundancy group for this group type. In order to avoid unnecessary collisions between competing management stations, `adjacent' retrievals of this object should give different index values. But in order to prevent leaks of unused indexes, it is acceptable to cycle through and report unused indexes again if all of the indexes have already been retrieved previously, yet some remain unused. So the retrieval of an index should not be considered a permanent longterm reservation. If there are no more unused group indexes available, the managed system should return 0. Note: 0 may be an acceptable group index on some managed systems. "
ceRedunReasonCategory	" This categorizes the specific switchover reason into one of several categories. "
ceRedunStateCategory	" This places the specific internal state into one of several categories of internal states which are significant for redundancy. "
ceRedunSwitchoverReasonDescr	" This is a string description for the specific switchover reason. "

ceRedunUsesGroupName	" Boolean to indicate whether this type of redundancy group uses the ceRedunGroupString object as a group name identifier. If it is reported as 'true', the ceRedunGroupString name must contain no internal spaces. If it's reported as 'false', the ceRedunGroupString object is just used as an optional description for the group rather than as the group name. "

CISCO-FTP-CLIENT-MIB

The MIB module for invoking Internet File Transfer Protoco (FTP) operations for network management purposes."

The following table lists the tables associated with this MIB:

MIB Name	Description
cfcRequestMaximum	" The maximum number of requests this system can hold in cfcRequestTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. When an attempt is made to create a new entry but the table is full, the oldest completed entry is bumped out and cfcRequestsBumped is incremented. Changing this number does not disturb existing requests that are not completed and bumps completed requests as necessary."
cfcRequests	" The current number of requests in cfcRequestTable."
cfcRequestsBumped	" The number of requests in cfcRequestTable that were bumped out to make room for a new request."
cfcRequestsHigh	" The highest number of requests in cfcRequestTable since this system was last initialized."

CISCO-FABRIC-HFR-MIB

Cisco Enhanced Benes fabric MIB module.This MIB module is used for managing/tracking the Ehanced Benes Fabric entities and/or fabric related configuration,state and statistics information.

The following table lists the tables associated with this MIB:

MIB Name	Description
cfhBundleDowned	" The current number of downed fabric bundles in the managed system."
cfhBundlePortTotalNumber	" The total number of fabric bundle ports in the managed system."
cfhBundleTotal	" The total number of fabric bundles in the managed system."
cfhGenBundleDownedLinkTrapEnable	" This object controls whether cfhBundleDownedLinkNotification traps should be generated for the downed fabric link in a specific fabric bundle. If the value of this object is 'true', the cfhBundleDownedLinkNotification traps will be generated when the number of downed links in fabric bundle has transitioned from 0 to 1 or from 1 to 0."
cfhGenBundleStateTrapEnable	" This object indicates whether cfhBundleStateNotification traps should be generated for fabric bundle operational status change. If the value of this object is 'true', cfhBundleStateNotification traps will be generated when the cfhBundleOperStatus state transition occurs."
cfhGenPlaneStateTrapEnable	" This object indicates whether cfhPlaneStateNotification traps should be generated for fabric plane operational status change. If the value of this object is 'true', cfhPlaneStateNotification traps will be generated when a fabric plane operational status transition occurs."
cfhPlaneAdminStatus	" This object controls whether the fabric plane should be brought 'down' or 'up'."
cfhPlaneDownedBundles	" The current number of downed fabric bundles in the fabric plane."
cfhPlaneOperStatus	" This object indicates the current fabric plane operational status. up - The plane is fully 'up' (i.e., the plane can pass both unicast and multicast traffic). down - The plane is fully 'down' (i.e., th plane can't pass both unicast and multicast traffic). mcastDown - The multicast state of the plane is 'down' (i.e., unicast traffic can pass though the plane but multicast traffic can't). oos - The plane is out of service (i.e., online diag detects the fabric transport media has problem in the plane)."
cfhPlaneStatsCounterDiscTime	" The value of sysUpTime on the most recent occasion at which all of fabric plane's counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
cfhPlaneStatsMulticastLostCells	" The accumulated number of multicast cell loss for this plane. The lost cells are ones that had to be dropped because of queue overflow, or some such reason."

cfhPlaneStatsRxCECells	" The accumulated number of correctable errored cells had been received by all link receivers for this plane."
cfhPlaneStatsRxDataCells	" The accumulated number of data cells have been received by all link receivers for this plane."
cfhPlaneStatsRxPECells	" The accumulated number of corrupted cells (e.g., parity error was detected in the cells) have been received by all fabric link receivers for this plane."
cfhPlaneStatsRxUCECells	" The accumulated number of uncorrectable errored cells had been received by all link receivers for this plane."
cfhPlaneStatsTxDataCells	" The accumulated number of data cells had been transmitted by all link transmitters for this plane."
cfhPlaneStatsUnicastLostCells	" The accumulated number of unicast cell loss for this plane. The lost cells are ones that had to be dropped because of queue overflow, or some such reason."
cfhPlaneTotalBundles	" The total number of fabric bundles in the fabric plane."

CISCO-FABRIC-MCAST-APPL-MIB

Fabric multicast resource MIB module.This MIB module is used for managing/tracking the fabric multicast resource application related information.

The following table lists the tables associated with this MIB:

MIB Name	Description
cfmaApplHighWaterInuseFGIDs	" The highest number of FGIDs that was in use by this application."
cfmaApplInuseFgids	" The number of FGIDs that are currently in use by this application."
cfmaApplName	" The name of this fabric multicast client application."
cfmaApplPoolId	" The fabric multicast resource pool id for the resource pool which is used by this application."

CISCO-FABRIC-MCAST-MIB

Fabric Multicast Resource MIB module.This MIB module is used for managing/tracking the fabric multicast resource related information.

The following table lists the tables associated with this MIB:

MIB Name	Description

cfmGenInfoHighWaterInuseFgids	" The highest number of FGIDs that was in use by all fabric multicast client applications in the managed system."
cfmGenInfoInuseFgids	" The current number of FGIDs that are currently in use by the managed system."
cfmGenInfoTotalFgids	" The total number of FGIDs resource are detected in the managed system."
cfmLrHighWaterInuseFgids	" The highest number of FGIDs that was in use by this logical router."
cfmLrInuseFgids	" The current number of FGIDs that are currently in use by this logical router."
cfmPoolHighWaterInuseFgids	" The highest number of FGIDs in this pool that was in use by the FGID clients from one or more logical routers."
cfmPoolInuseFgids	" The current number of FGIDs in this pool that are currently in use by the FGID clients from one or more logical routers."
cfmPoolName	" The object to indicate FGID pool name."
cfmPoolTotalFgids	" The total number of FGIDs in this pool. The total size might be dynamically adjusted based on the utilization of each pool or if a fabric multicast resource related entity is added or removed (e.g., add a new fabric rack or upgrade an old fabric rack to new fabric rack)."
cfmPoolType	" The object to indicate FGID pool type. shared(1) - the pool is shared by multiple types of FGID clients. dedicated(2) - the pool is dedicated for a specific type of client to use. The dedicated pool is normally used by a critical client to prevent processes deadlock during system initialization or restart."

CISCO-HSRP-MIB

The MIB module provides a means to monitor and configure the Cisco IOS proprietary Hot Standby Router Protocol (HSRP). Cisco HSRP protocol is defined in RFC2281.

The following table lists the tables associated with this MIB:

MIB Name	Description
cHsrpConfigTimeout	" The amount of time in minutes a row in cHsrpGrpTable can remain in a state other than active before being timed out."

CISCO-IP-ADDRESS-POOL-MIB

This MIB modules defines objects that describe common aspects of IP address pools.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciapGlobalNotifyEnable	" This object specifies whether the IP address pool manager generates notifications defined by this MIB module."
ciapPoolAddressesFree	" This object indicates the number of available IP addresses or prefixes in this IP address pool."
ciapPoolThresholdFalling	" This object specifies the falling threshold for the in-use gauge corresponding to this IP address pool, which must have a value less than or equal to the corresponding instance of ciapPoolThresholdRising. If this value is '0' and the corresponding instance of ciapPoolThresholdRising is '0', then the IP address pool manager does not monitor this IP address pool for threshold crossing events. The value of ciapGlobalThresholdFalling.0 specifies the default value for newly created instances of this object. For more detail, see the description of IP address pool threshold monitoring provided by the descriptive text associated with the MODULE-IDENTITY statement."
ciapPoolThresholdUnits	" This object specifies the units for the corresponding instances of ciapPoolThresholdRising and ciapPoolThresholdFalling. The value of ciapGlobalThresholdUnits.0 specifies the default value for newly created instances of this object."
ciapPoolType	" This object specifies the how the system uses this IP address pool: 'other' The implementation of the MIB module does not recognize this IP address pool's type. 'shared' The system uses this IP address pool regardless of the entity (e.g., IPCP, IPsec, DHCP) allocating IP addresses from this IP address pool. Sometimes we use the term 'untyped pool' to refer to an IP address pool used in this manner. 'local' The system restricts the use this IP address pool to assign IP addresses to peers when establishing a connection (e.g., PPP and IPsec) to the system. 'dhcp' The system restricts the use of this IP address pool to a DHCP server."

CISCO-IF-EXTENSION-MIB

A MIB module for extending the IF-MIB (RFC2863) to add objects which provide additional information about interfaces not available in other MIBS.This MIB replaces the OLD-CISCO-INTERFACES-MIB.

The following table lists the tables associated with this MIB:

MIB Name	Description
cieIfCarrierTransitionCount	" Number of times interface saw the carrier signal transition. For example, if a T1 line is unplugged, then framer will detect the loss of signal (LOS) on the line and will count it as a transition. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfInterfaceDiscontinuityTime."
cieIfContextName	" The ContextName denotes the interface 'context' and is used to logically separate the MIB management. RFC 2571 and RFC 2737 describe this approach. When the agent supports a different SNMP context, as detailed in RFC 2571 and RFC 2737, for different interfaces, then the value of this object specifies the context name used for this interface."
cieIfInAbortErrs	" Number of input packets which were dropped because the receiver cancelled. Examples of this could be when a cancel sequence cancelled the input frame or when there is a collision in an ethernet segment. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfInFramingErrs	" The number of input packets on a physical interface which were misaligned or had framing errors. This happens when the format of the incoming packet on a physical interface is incorrect. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfInGiantsErrs	" The number of input packets on a particular physical interface which were dropped as they were larger than the ifMtu (largest permitted size of a packet which can be sent/received on an interface). Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfInIgnored	" The number of input packets which were simply ignored by this physical interface due to insufficient resources to handle the incoming packets. For example, this could indicate that the input receive buffers are not available or that the receiver lost a packet. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."

cieIfInOctetRate	" By default, this is the five minute exponentially-decayed moving average of the inbound octet rate for this interface. However, if the corresponding instance of cieIfInterval is instantiated with a value which specifies an interval different from 5-minutes, then cieIfInOctetRate is the exponentially-decayed moving average of inbound octet rate over this different time interval."
cieIfInOverrunErrs	" The number of input packets which arrived on a particular physical interface which were too quick for the hardware to receive and hence the receiver ran out of buffers. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfInPktRate	" By default, this is the five minute exponentially-decayed moving average of the inbound packet rate for this interface. However, if the corresponding instance of cieIfInterval is instantiated with a value which specifies an interval different from 5-minutes, then cieIfInPktRate is the exponentially-decayed moving average of inbound packet rate over this different time interval."
cieIfInputQueueDrops	" The number of input packets which were dropped. Some reasons why this object could be incremented are: o Input queue is full. o Errors at the receiver hardware while receiving the packet. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfInRuntsErrs	" The number of packets input on a particular physical interface which were dropped as they were smaller than the minimum allowable physical media limit. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."
cieIfKeepAliveEnabled	" A keepalive is a small, layer-2 message that is transmitted by a network device to let directly-connected network devices know of its presence. This object returns 'true' if keepalives are enabled on this interface. If keepalives are not enabled, 'false' is returned. Setting this object to TRUE or FALSE enables or disables (respectively) keepalive on this interface."
cieIfMtu	" The MTU configured by the administrator. This object is exactly same as 'ifMtu' in ifTable from IF-MIB for the same ifIndex value , except that it is configurable by the administrator. For more description of this object refer to 'ifMtu' in IF-MIB."

cieIfOperStatusCause	" This object represents the detailed operational cause reason for the current operational state of the interface. The current operational state of the interface is given by the 'ifOperStatus' defined in IF-MIB. The corresponding instance of 'cieIfOperStatusCauseDescr' must be used to get the information about the operational cause value mentioned in this object. For interfaces whose 'ifOperStatus' is 'down' the objects 'cieIfOperStatusCause' and 'cieIfOperStatusCauseDescr' together provides the information about the operational cause reason and the description of the cause. The value of this object will be 'none' for all the 'ifOperStatus' values except for 'down'. Its value will be one status cause defined in the 'IfOperStatusReason' textual convention if 'ifOperStatus' is 'down'. The value of this object will be 'other' if the operational status cause is not one defined in 'IfOperStatusReason'."
cieIfOperStatusCauseDescr	" The description for the cause of current operational state of the interface, given by the object 'cieIfOperStatusCause'. For an interface whose 'ifOperStatus' is not 'down' the value of this object will be 'none'."
cieIfOutOctetRate	" By default, this is the five minute exponentially-decayed moving average of the outbound octet rate for this interface. However, if the corresponding instance of cieIfInterval is instantiated with a value which specifies an interval different from 5-minutes, then cieIfOutOctetRate is the exponentially-decayed moving average of outbound octet rate over this different time interval."
cieIfOutPktRate	" By default, this is the five minute exponentially-decayed moving average of the outbound packet rate for this interface. However, if the corresponding instance of cieIfInterval is instantiated with a value which specifies an interval different from 5-minutes, then cieIfOutPktRate is the exponentially-decayed moving average of outbound packet rate over this different time interval."
cieIfOutputQueueDrops	" This object indicates the number of output packets dropped by the interface even though no error had been detected to prevent them being transmitted. The packet could be dropped for many reasons, which could range from the interface being down to errors in the format of the packet. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfPacketDiscontinuityTime."

cieIfResetCount	" The number of times the interface was internally reset and brought up. Some of the actions which can cause this counter to increment are : o Bringing an interface up using the interface CLI command. o Clearing the interface with the exec CLI command. o Bringing the interface up via SNMP. Discontinuities in the value of this variable can occur at re-initialization of the management system, and at other times as indicated by the values of cieIfInterfaceDiscontinuityTime."
cieIfStateChangeReason	" This object displays a human-readable textual string which describes the cause of the last state change of the interface. Examples of the values this object can take are: o 'Lost Carrier' o 'administratively down' o 'up' o 'down'"

CISCO-IPSEC-MIB

The MIB module for modeling Cisco-specific IPsec attributes.

The following table lists the tables associated with this MIB:

MIB Name	Description
cipsMaxSAs	" The maximum number of IPsec Security Associations that can be established on this managed entity. If no theoretical limit exists, this returns value 0. Not affected by any CLI operation."
cipsNumCETCryptomapSets	" The number of static Cryptomap Sets that have at least one CET cryptomap element as a member of the set."
cipsNumDynamicCryptomapSets	" The number of dynamic IPSec Policy templates (called 'dynamic cryptomap templates') configured on the managed entity."
cipsNumStaticCryptomapSets	" The number of Cryptomap Sets that are are fully configured. Statically defined cryptomap sets are ones where the operator has fully specified all the parameters required set up IPSec Virtual Private Networks (VPNs)."
cipsNumTEDCryptomapSets	" The number of static Cryptomap Sets that have at least one dynamic cryptomap template bound to them which has the Tunnel Endpoint Discovery (TED) enabled."
cipsSALifesize	" The default lifesize in KBytes assigned to an SA as a global policy (unless overridden in cryptomap definition)"
cipsSALifetime	" The default lifetime (in seconds) assigned to an SA as a global policy (maybe overridden in specific cryptomap definitions)."

CISCO-CDP-MIB

The MIB module for management of the Cisco Discovery Protocol in Cisco devices."

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoCdpMIB	" The MIB module for management of the Cisco Discovery Protocol in Cisco devices."

CISCO-ENTITY-ASSET-MIB

Monitor the asset information of items in the ENTITY-MIB (RFC 2037) entPhysical table.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoEntityAssetMIB	" Monitor the asset information of items in the ENTITY-MIB (RFC 2037) entPhysical table."

CISCO-ENTITY-FRU-CONTROL-MIB

The CISCO-ENTITY-FRU-CONTROL-MIB is used to monitor and configure operational status of Field Replaceable Units (FRUs) and other managable physical entities of the system listed in the Entity-MIB (RFC 2737) entPhysicalTable.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoEntityFRUControlMIB	" The CISCO-ENTITY-FRU-CONTROL-MIB is used to monitor and configure operational status of Field Replaceable Units (FRUs) and other managable physical entities of the system listed in the Entity-MIB (RFC 2737) entPhysicalTable. FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc."

CISCO-FABRIC-HFR-MIB

Cisco Enhanced Benes fabric MIB module. This MIB module is used for managing/tracking the Ehanced Benes Fabric entities and/or fabric.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoFabricHfrMIB	" Cisco Enhanced Benes fabric MIB module. This MIB module is used for managing/tracking the Ehanced Benes Fabric entities and/or fabric related configuration, state and statistics information. The fabric entities relationship is shown as follows: Acronyms and terms: RP - Routing processor. DRP - Distributed Route Processor. LC - Line card. SFE - switch fabric element. SFE port - the port of SFE contains a transmitter and/or receiver to transmit and/or receive data from backplane. fabric link - Fabric link. +-+ +-+ |T1+==========> +R| +-+ single fabric link +-+ A fabric link contains a transmitter T and receiver R. The transmitter T is in the source SFE port of the fabric link and the receiver R is in the destination SFE port of the fabric link. OIM - Optical Interface Module. fabric bundle - Fabric bundle is a cable that contains one or more fabric links for transferring data between fabric cards. +-+ +-+ |A+==========/========== +B| +-+ 1..N fabric links +-+ A fabric bundle cable contains 1 to N fabric links. One end of the fabric bundle cable is plugged into the fabric bundle port A of fabric card in Line card rack and the other end is plugged into the fabric bundle port B on a OIM of fabric rack for the high speed data transfer between fabric bundle port A and B. ingressq - a switch fabric element which queues/segments packets into cells and sends them into fabric. fabricq - a switch fabric element which resequences and reassembles cells from fabric into packets and forwarding them to the egress interface related hardware. fabric plane - Fabric plane is a path from a set of ingressqs in a RP/DRP or LC card to a set of fabricqs in other RP/DRP or LC cards for transferring data between RP, DRP, and LC cards."

CISCO-FABRIC-MCAST-MIB

Fabric Multicast Resource MIB module.This MIB module is used for managing/tracking the fabric multicast resource related information.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoFabricMcastMIB	" Fabric Multicast Resource MIB module. This MIB module is used for managing/tracking the fabric multicast resource related information. Acronyms and terms: FGID - Fabric Multicast Group Identifier. LR - Logical router."

CISCO-FLASH-MIB

This MIB provides for the management of Cisco Flash Devices.

following table lists the tables associated with this MIB:

MIB Name	Description
ciscoFlashChipCode	" Manufacturer and device code for a chip. Lower byte will contain the device code. Upper byte will contain the manufacturer code. If a chip code is unknown because it could not be queried out of the chip, the value of this object will be 00:00. Since programming algorithms differ from chip type to chip type, this chip code should be used to determine which algorithms to use (and thereby whether the chip is supported in the first place)."
ciscoFlashChipDescr	" Flash chip name corresponding to the chip code. The name will contain the manufacturer and the chip type. It will be of the form : Intel 27F008SA. In the case where a chip code is unknown, this object will be an empty (NULL) string. In the case where the chip code is known but the chip is not supported by the system, this object will be an empty (NULL) string. A management station is therefore expected to use the chip code and the chip description in conjunction to provide additional information whenever the ciscoFlashPartitionStatus object has the readOnly(1) value."

ciscoFlashChipEraseRetries	" This object will provide a cumulative count (since last system boot up or initialization) of the number of erase retries that were done in the chip. Typically, a maximum of 2000 retries are done in a single erase zone (which may be a full chip or a portion, depending on the chip technology) before flagging an erase error. A management station is expected to get this object for each chip in a partition after an erase failure in that partition. To keep a track of retries for a given erase operation, the management station would have to retrieve the values for the concerned chips before and after any erase operation. Note that erase may be done through an independent command, or through a copy-to-flash command."
ciscoFlashChipMaxEraseRetries	" The maximum number of erase retries done within an erase sector before declaring an erase failure."
ciscoFlashChipMaxWriteRetries	" The maximum number of write retries done at any single location before declaring a write failure."
ciscoFlashChipWriteRetries	" This object will provide a cumulative count (since last system boot up or initialization) of the number of write retries that were done in the chip. If no writes have been done to Flash, the count will be zero. Typically, a maximum of 25 retries are done on a single location before flagging a write error. A management station is expected to get this object for each chip in a partition after a write failure in that partition. To keep a track of retries for a given write operation, the management station would have to retrieve the values for the concerned chips before and after any write operation."
ciscoFlashDeviceCard	" This object will point to an instance of a card entry in the cardTable. The card entry will give details about the card on which the Flash device is actually located. For most systems, this is usually the main processor board. On the AGS+ systems, Flash is located on a separate multibus card such as the MC. This object will therefore be used to essentially index into cardTable to retrieve details about the card such as cardDescr, cardSlotNumber, etc."
ciscoFlashDeviceChipCount	" Total number of chips within the Flash device. The purpose of this object is to provide information upfront to a management station on how much chip info to expect and possibly help double check the chip index against an upper limit when randomly retrieving chip info for a partition."

ciscoFlashDeviceController	" Flash device controller. The h/w card that actually controls Flash read/write/erase. Relevant for the AGS+ systems where Flash may be controlled by the MC+, STR or the ENVM cards, cards that may not actually contain the Flash chips. For systems that have removable PCMCIA flash cards that are controlled by a PCMCIA controller chip, this object may contain a description of that controller chip. Where irrelevant (Flash is a direct memory mapped device accessed directly by the main processor), this object will have an empty (NULL) string."
ciscoFlashDeviceDescr	" Description of a Flash device. The description is meant to explain what the Flash device and its purpose is. Current values are: System flash - for the primary Flash used to store full system images. Boot flash - for the secondary Flash used to store bootstrap images. The ciscoFlashDeviceDescr, ciscoFlashDeviceController (if applicable), and ciscoFlashPhyEntIndex objects are expected to collectively give all information about a Flash device. The device description will always be available for a removable device, even when the device has been removed."
ciscoFlashDeviceInitTime	" System time at which device was initialized. For fixed devices, this will be the system time at boot up. For removable devices, it will be the time at which the device was inserted, which may be boot up time, or a later time (if device was inserted later). If a device (fixed or removable) was repartitioned, it will be the time of repartitioning. The purpose of this object is to help a management station determine if a removable device has been changed. The application should retrieve this object prior to any operation and compare with the previously retrieved value. Note that this time will not be real time but a running time maintained by the system. This running time starts from zero when the system boots up. For a removable device that has been removed, this value will be zero."
ciscoFlashDeviceMaxPartitions	" Max number of partitions supported by the system for this Flash device. Default will be 1, which actually means that partitioning is not supported. Note that this value will be defined by system limitations, not by the flash device itself (for eg., the system may impose a limit of 2 partitions even though the device may be large enough to be partitioned into 4 based on the smallest partition unit supported). On systems that execute code out of Flash, partitioning is a way of creating multiple file systems in the Flash device so that writing into or erasing of one file system can be done while executing code residing in another file system. For systems executing code out of DRAM, partitioning gives a way of sub-dividing a large Flash device for easier management of files."

ciscoFlashDeviceMinPartitionSize	" This object will give the minimum partition size supported for this device. For systems that execute code directly out of Flash, the minimum partition size needs to be the bank size. (Bank size is equal to the size of a chip multiplied by the width of the device. In most cases, the device width is 4 bytes, and so the bank size would be four times the size of a chip). This has to be so because all programming commands affect the operation of an entire chip (in our case, an entire bank because all operations are done on the entire width of the device) even though the actual command may be localized to a small portion of each chip. So when executing code out of Flash, one needs to be able to write and erase some portion of Flash without affecting the code execution. For systems that execute code out of DRAM or ROM, it is possible to partition Flash with a finer granularity (for eg., at erase sector boundaries) if the system code supports such granularity. This object will let a management entity know the minimum partition size as defined by the system. If the system does not support partitioning, the value will be equal to the device size in ciscoFlashDeviceSize. The maximum number of partitions that could be configured will be equal to the minimum of ciscoFlashDeviceMaxPartitions and (ciscoFlashDeviceSize / ciscoFlashDeviceMinPartitionSize). If the total size of the flash device is greater than the maximum value reportable by this object then this object should report its maximum value(4,294,967,295) and ciscoFlashDeviceMinPartitionSizeExtended must be used to report the flash device's minimum partition size."
ciscoFlashDeviceMinPartitionSizeExtended	" This object provides the minimum partition size supported for this device. This object is a 64-bit version of ciscoFlashDeviceMinPatitionSize."
ciscoFlashDeviceName	" Flash device name. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name. The system has a concept of a default device. This would be the primary or most used device in case of multiple devices. The system directs an operation to the default device whenever a device name is not specified. The device name is therefore mandatory except when the operation is being done on the default device, or, the system supports only a single Flash device. The device name will always be available for a removable device, even when the device has been removed."

ciscoFlashDeviceNameExtended	" Extended Flash device name whose size can be upto 255 characters. This name is used to refer to the device within the system. Flash operations get directed to a device based on this name. The system has a concept of a default device. This would be the primary or most used device in case of multiple devices. The system directs an operation to the default device whenever a device name is not specified. The device name is therefore mandatory except when the operation is being done on the default device, or, the system supports only a single Flash device. The device name will always be available for a removable device, even when the device has been removed."
ciscoFlashDevicePartitions	" Flash device partitions actually present. Number of partitions cannot exceed the minimum of ciscoFlashDeviceMaxPartitions and (ciscoFlashDeviceSize / ciscoFlashDeviceMinPartitionSize). Will be equal to at least 1, the case where the partition spans the entire device (actually no partitioning). A partition will contain one or more minimum partition units (where a minimum partition unit is defined by ciscoFlashDeviceMinPartitionSize)."
ciscoFlashDeviceProgrammingJumper	" This object gives the state of a jumper (if present and can be determined) that controls the programming voltage called Vpp to the Flash device. Vpp is required for programming (erasing and writing) Flash. For certain older technology chips it is also required for identifying the chips (which in turn is required to identify which programming algorithms to use; different chips require different algorithms and commands). The purpose of the jumper, on systems where it is available, is to write protect a Flash device. On most of the newer remote access routers, this jumper is unavailable since users are not expected to visit remote sites just to install and remove the jumpers when upgrading software in the Flash device. The unknown(3) value will be returned for such systems and can be interpreted to mean that a programming jumper is not present or not required on those systems. On systems where the programming jumper state can be read back via a hardware register, the installed(1) or notInstalled(2) value will be returned. This object is expected to be used in conjunction with the ciscoFlashPartitionStatus object whenever that object has the readOnly(1) value. In such a case, this object will indicate whether the programming jumper is a possible reason for the readOnly state."

ciscoFlashDeviceRemovable	" Whether Flash device is removable. Generally, only PCMCIA Flash cards will be treated as removable. Socketed Flash chips and Flash SIMM modules will not be treated as removable. Simply put, only those Flash devices that can be inserted or removed without opening the hardware casing will be considered removable. Further, removable Flash devices are expected to have the necessary hardware support - 1. on-line removal and insertion 2. interrupt generation on removal or insertion."
ciscoFlashDeviceSize	" Total size of the Flash device. For a removable device, the size will be zero if the device has been removed. If the total size of the flash device is greater than the maximum value reportable by this object then this object should report its maximum value(4,294,967,295) and ciscoFlashDeviceSizeExtended must be used to report the flash device's size."
ciscoFlashDeviceSizeExtended	" Total size of the Flash device. For a removable device, the size will be zero if the device has been removed. This object is a 64-bit version of ciscoFlashDeviceSize."
ciscoFlashDevicesSupported	" Number of Flash devices supported by the system. If the system does not support any Flash devices, this MIB will not be loaded on that system. The value of this object will therefore be atleast 1."
ciscoFlashFileChecksum	" File checksum stored in the file header. This checksum is computed and stored when the file is written into Flash. It serves to validate the data written into Flash. Whereas the system will generate and store the checksum internally in hexadecimal form, this object will provide the checksum in a string form. The checksum will be available for all valid and invalid-checksum files."
ciscoFlashFileName	" Flash file name as specified by the user copying in the file. The name should not include the colon (:) character as it is a special separator character used to delineate the device name, partition name, and the file name."
ciscoFlashFileSize	" Size of the file in bytes. Note that this size does not include the size of the filesystem file header. File size will always be non-zero."
ciscoFlashFileStatus	" Status of a file. A file could be explicitly deleted if the file system supports such a user command facility. Alternately, an existing good file would be automatically deleted if another good file with the same name were copied in. Note that deleted files continue to occupy prime Flash real estate. A file is marked as having an invalid checksum if any checksum mismatch was detected while writing or reading the file. Incomplete files (files truncated either because of lack of free space, or a network download failure) are also written with a bad checksum and marked as invalid."
ciscoFlashFileType	" Type of the file."
ciscoFlashMIB	" This MIB provides for the management of Cisco Flash Devices."

ciscoFlashPartitionChecksumAlgorithm	" Checksum algorithm identifier for checksum method used by the file system. Normally, this would be fixed for a particular file system. When a file system writes a file to Flash, it checksums the data written. The checksum then serves as a way to validate the data read back whenever the file is opened for reading. Since there is no way, when using TFTP, to guarantee that a network download has been error free (since UDP checksums may not have been enabled), this object together with the ciscoFlashFileChecksum object provides a method for any management station to regenerate the checksum of the original file on the server and compare checksums to ensure that the file download to Flash was error free. simpleChecksum represents a simple 1s complement addition of short word values. Other algorithm values will be added as necessary."
ciscoFlashPartitionEndChip	" Chip sequence number of last chip in partition. Used as an index into the chip table."
ciscoFlashPartitionFileCount	" Count of all files in a flash partition. Both good and bad (deleted or invalid checksum) files will be included in this count."
ciscoFlashPartitionFileNameLength	" Maximum file name length supported by the file system. Max file name length will depend on the file system implemented. Today, all file systems support a max length of at least 48 bytes. A management entity must use this object when prompting a user for, or deriving the Flash file name length."
ciscoFlashPartitionFreeSpace	" Free space within a Flash partition. Note that the actual size of a file in Flash includes a small overhead that represents the file system's file header. Certain file systems may also have a partition or device header overhead to be considered when computing the free space. Free space will be computed as total partition size less size of all existing files (valid/invalid/deleted files and including file header of each file), less size of any partition header, less size of header of next file to be copied in. In short, this object will give the size of the largest file that can be copied in. The management entity will not be expected to know or use any overheads such as file and partition header lengths, since such overheads may vary from file system to file system. Deleted files in Flash do not free up space. A partition may have to be erased in order to reclaim the space occupied by files. If the free space within a flash partition is greater than the maximum value reportable by this object then this object should report its maximum value(4,294,967,295) and ciscoFlashPartitionFreeSpaceExtended must be used to report the flash partition's free space."

ciscoFlashPartitionFreeSpaceExtended	" Free space within a Flash partition. Note that the actual size of a file in Flash includes a small overhead that represents the file system's file header. Certain file systems may also have a partition or device header overhead to be considered when computing the free space. Free space will be computed as total partition size less size of all existing files (valid/invalid/deleted files and including file header of each file), less size of any partition header, less size of header of next file to be copied in. In short, this object will give the size of the largest file that can be copied in. The management entity will not be expected to know or use any overheads such as file and partition header lengths, since such overheads may vary from file system to file system. Deleted files in Flash do not free up space. A partition may have to be erased in order to reclaim the space occupied by files. This object is a 64-bit version of ciscoFlashPartitionFreeSpace"
ciscoFlashPartitionName	" Flash partition name used to refer to a partition by the system. This can be any alpha-numeric character string of the form AAAAAAAAnn, where A represents an optional alpha character and n a numeric character. Any numeric characters must always form the trailing part of the string. The system will strip off the alpha characters and use the numeric portion to map to a partition index. Flash operations get directed to a device partition based on this name. The system has a concept of a default partition. This would be the first partition in the device. The system directs an operation to the default partition whenever a partition name is not specified. The partition name is therefore mandatory except when the operation is being done on the default partition, or the device has just one partition (is not partitioned)."
ciscoFlashPartitionNeedErasure	" This object indicates whether a partition requires erasure before any write operations can be done in it. A management station should therefore retrieve this object prior to attempting any write operation. A partition requires erasure after it becomes full free space left is less than or equal to the (filesystem file header size). A partition also requires erasure if the system does not find the existence of any file system when it boots up. The partition may be erased explicitly through the erase(5) command, or by using the copyToFlashWithErase(1) command. If a copyToFlashWithoutErase(2) command is issued when this object has the TRUE value, the command will fail."
ciscoFlashPartitionSize	" Flash partition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize. If the size of the flash partition is greater than the maximum value reportable by this object then this object should report its maximum value(4,294,967,295) and ciscoFlashPartitionSizeExtended must be used to report the flash partition's size."

ciscoFlashPartitionSizeExtended	" Flash partition size. It should be an integral multiple of ciscoFlashDeviceMinPartitionSize. If there is a single partition, this size will be equal to ciscoFlashDeviceSize. This object is a 64-bit version of ciscoFlashPartitionSize"
ciscoFlashPartitionStartChip	" Chip sequence number of first chip in partition. Used as an index into the chip table."
ciscoFlashPartitionStatus	" Flash partition status can be : * readOnly if device is not programmable either because chips could not be recognized or an erroneous mismatch of chips was detected. Chip recognition may fail either because the chips are not supported by the system, or because the Vpp voltage required to identify chips has been disabled via the programming jumper. The ciscoFlashDeviceProgrammingJumper, ciscoFlashChipCode, and ciscoFlashChipDescr objects can be examined to get more details on the cause of this status * runFromFlash (RFF) if current image is running from this partition. The ciscoFlashPartitionUpgradeMethod object will then indicate whether the Flash Load Helper can be used to write a file to this partition or not. * readWrite if partition is programmable."
ciscoFlashPartitionUpgradeMethod	" Flash partition upgrade method, ie., method by which new files can be downloaded into the partition. FLH stands for Flash Load Helper, a feature provided on run-from-Flash systems for upgrading Flash. This feature uses the bootstrap code in ROMs to help in automatic download. This object should be retrieved if the partition status is runFromFlash(2). If the partition status is readOnly(1), the upgrade method would depend on the reason for the readOnly status. For eg., it may simply be a matter of installing the programming jumper, or it may require execution of a later version of software that supports the Flash chips. unknown - the current system image does not know how Flash can be programmed. A possible method would be to reload the ROM image and perform the upgrade manually. rxbootFLH - the Flash Load Helper is available to download files to Flash. A copy-to-flash command can be used and this system image will automatically reload the Rxboot image in ROM and direct it to carry out the download request. direct - will be done directly by this image."
ciscoFlashPhyEntIndex	" This object indicates the physical entity index of a physical entity in entPhysicalTable which the flash device actually located."

CISCO-AAL5-EXT-MIB

This MIB is the RFC 1695 extension for Cisco product. It provides the additional AAL5 performance statistic of a VCC from RFC 1695.

The following table lists the tables associated with this MIB:

MIB Name	Description
ciscoMgmt 9999	The number of AAL5 SAR cells dropped at the transmit side of this AAL5 VCC at the interface associated with an AAL5 entity."

CISCO-OTN-IF-MIB

This MIB module defines the managed objects for physical layer characteristics of DWDM optical channel interfaces and performance statistics objects for protocol specific error counters in DWDM optical devices.

The following table lists the tables associated with this MIB:

MIB Name	Description

ciscoOtnIfMIB	" This MIB module defines the managed objects for physical layer characteristics of DWDM optical channel interfaces and performance statistics objects for protocol specific error counters in DWDM optical devices. Performance monitoring (PM) parameters are used by service providers to gather, store, set thresholds for and report performance data for early detection of problems. Thresholds are used to set error levels for each PM parameter. During the accumulation cycle, if the current value of a performance monitoring parameter reaches or exceeds its corresponding threshold value, a threshold crossing alarm (TCA) is generated. The TCAs provide early detection of performance degradation. The definitions contained herein are based on the OTN specifications in ITU-T G.872[ITU-T G.872], G.709 [ITU-T G.709], G.798[ITU-T G.798], G.874[ITU-T G.874], and G.874.1[ITU-T G.874.1]. Glossary: OTN : Optical Transport Network (ITU-T G.709). FEC : Forward Error Correction. PM : Performance Monitor. DWDM : Dense Wavelength Division Multiplexing. FE : Farend or client side of the interface. NE : Nearend or trunk side of the interface. ADM : Add Drop Multiplexer. OCH : Optical Channel. OTS : Optical Transport Section. OMS : Optical Multiplex Section. TCA : Threshold Crossing Alarm. OSC : Optical Supervisory Channel. DCU : Dispersion Compensation Unit. EXP : Express Channel. OSNR : Optical singal to noise ratio. OTU : Optical Channel Transport Unit. ODU : Optical Channel Data Unit."

CISCO-RTTMON-MIB

This module defines a MIB for Round Trip Time (RTT) monitoring of a list of targets, using avariety of protocols.

The following table lists the tables associated with this MIB:

MIB Name	Description

ciscoRttMonMIB	" This module defines a MIB for Round Trip Time (RTT) monitoring of a list of targets, using a variety of protocols.
rttMonApplResponder	" Enable or disable RTR responder on the router."
rttMonApplSupportedProtocolsValid	" This object defines the supported 'RttMonProtocol' protocols."
rttMonApplSupportedRttTypesValid	" This object defines the supported 'RttMonRttType' types."

CISCO-SYSLOG-MIB

The MIB module to describe and store the system messages generated by the IOS and any other OS which supports syslogs."

The following table lists the tables associated with this MIB:

MIB Name	Description

ciscoSyslogMIB	" The MIB module to describe and store the system messages generated by the IOS and any other OS which supports syslogs."
CISCO-TCP-MIB	" An extension to the IETF MIB module for managing TCP implementations"
ciscoTcpConnElapsed	" Amount of time this TCP connection has been established."
ciscoTcpConnFastRetransPkts	" The total number of packets retransmitted using an advanced algorithm such as Fast Retransmit or Selective Acknowledgement - that is, the number of TCP segments transmitted containing one or more previously transmitted octets."
ciscoTcpConnInBytes	" Number of bytes that have been input on this TCP connection."
ciscoTcpConnInPkts	" Number of packets that have been input on this TCP connection."
ciscoTcpConnOutBytes	" Number of bytes that have been output on this TCP connection."
ciscoTcpConnOutPkts	" Number of packets that have been output on this TCP connection."
ciscoTcpConnRetransPkts	" The total number of packets retransmitted due to a timeout - that is, the number of TCP segments transmitted containing one or more previously transmitted octets."
ciscoTcpConnRto	" The current value used by a TCP implementation for the retransmission timeout."
ciscoTcpConnSRTT	" `Smoothed' round-trip time for this TCP connection."
ciscoTcpMIB	" An extension to the IETF MIB module for managing TCP implementations"
CISCO-SYSLOG-MIB	" The MIB module to describe and store the system messages generated by the IOS and any other OS which supports syslogs."
clogHistFacility	" Name of the facility that generated this message. For example: 'SYS'."
clogHistMsgName	" A textual identification for the message type. A facility name in conjunction with a message name uniquely identifies a message type."
clogHistMsgsFlushed	" The number of entries that have been removed from the clogHistoryTable in order to make room for new entries. This object can be utilized to determine whether your polling frequency on the history table is fast enough and/or the size of your history table is large enough such that you are not missing messages."
clogHistMsgText	" The text of the message. If the text of the message exceeds 255 bytes, the message will be truncated to 254 bytes and a '*' character will be appended - indicating that the message has been truncated."
clogHistSeverity	" The severity of the message."
clogHistTableMaxLength	" The upper limit on the number of entries that the clogHistoryTable may contain. A value of 0 will prevent any history from being retained. When this table is full, the oldest entry will be deleted and a new one will be created."

clogHistTimestamp	" The value of sysUpTime when this message was generated."
clogMaxSeverity	" Indicates which syslog severity levels will be processed. Any syslog message with a severity value greater than this value will be ignored by the agent. note: severity numeric values increase as their severity decreases, e.g. 'error' is more severe than 'debug'."
clogMsgDrops	" The number of syslog messages which could not be processed due to lack of system resources. Most likely this will occur at the same time that syslog messages are generated to indicate this lack of resources. Increases in this object's value may serve as an indication that system resource levels should be examined via other mib objects. A message that is dropped will not appear in the history table and no notification will be sent for this message."
clogMsgIgnores	" The number of syslog messages which were ignored. A message will be ignored if it has a severity value greater than clogMaxSeverity."
clogNotificationsEnabled	" Indicates whether clogMessageGenerated notifications will or will not be sent when a syslog message is generated by the device. Disabling notifications does not prevent syslog messages from being added to the clogHistoryTable."
clogNotificationsSent	" The number of clogMessageGenerated notifications that have been sent. This number may include notifications that were prevented from being transmitted due to reasons such as resource limitations and/or non-connectivity. If one is receiving notifications, one can periodically poll this object to determine if any notifications were missed. If so, a poll of the clogHistoryTable might be appropriate."

CISCO-IETF-FRR-MIB

This MIB module contains managed object definitions for MPLS Fast Reroute (FRR) as defined in:Pan, P., Gan, D., Swallow, G.,Vasseur, J.Ph., Cooper, D., Atlas, A., Jork, M., Fast Reroute Techniques in RSVP-TE, draft-ietf-mpls-rsvp-lsp-fastreroute-00.txt, January 2002."

The following table lists the tables associated with this MIB:

MIB Name	Description
cmplsFrrActProtectedIfs	" Indicates the number of interfaces currently being protected by the FRR feature if mplsFrrConstProtectionMethod is set to facilityBackup(1), otherwise this value should return 0 to indicate that LSPs traversing any interface may be protected. This value MUST be less than or equal to mplsFrrConfIfs."

cmplsFrrActProtectedLSPs	" Indicates the number of LSPs currently protected by the FRR feature. If mplsFrrConstProtectionMethod is set to facilityBackup(1)this object MUST return 0."
cmplsFrrActProtectedTuns	" Indicates the number of bypass tunnels indicated in mplsFrrConfProtectingTuns whose operStatus is up(1) indicating that they are currently protecting facilities on this LSR using the FRR feature. This object MUST return 0 if mplsFrrConstProtectionMethod is set to facilityBackup(1)."
cmplsFrrConfProtectingTuns	" Indicates the number of bypass tunnels configured to protect facilities on this LSR using the FRR feature if mplsFrrConstProtectionMethod is set to facilityBackup(1), otherwise this value MUST return 0."
cmplsFrrConstBandwidth	" This variable represents the bandwidth for detour LSPs of this tunnel, in units of thousands of bits per second (Kbps)."
cmplsFrrConstExclAllAffinity	" A link satisfies the exclude-all constraint if and only if the link contains none of the administrative groups specified in the constraint." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
cmplsFrrConstHoldingPrio	" Indicates the holding priority for detour LSP." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001"
cmplsFrrConstHopLimit	" The maximum number of hops that the detour LSP may traverse." REFERENCE " Pan, P., Gan, D., Swallow, G., Vasseur, J.Ph., Cooper, D., Atlas, A., Jork, M., Fast Reroute Techniques in RSVP-TE, draft- ietf-mpls-rsvp-lsp-fastreroute-00.txt, January 2002. Work in progress."
cmplsFrrConstInclAllAffinity	" A link satisfies the include-all constraint if and only if the link contains all of the administrative groups specified in the constraint." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
cmplsFrrConstInclAnyAffinity	" A link satisfies the include-any constraint if and only if the constraint is zero, or the link and the constraint have a resource class in common." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
cmplsFrrConstNumProtectedTunOnIf	" The number of tunnels protected on this interface."
cmplsFrrConstNumProtectingTunOnIf	" The number of backup tunnels protecting the specified interface."

cmplsFrrConstProtectionMethod	" Indicates which protection method is to be used for fast reroute. Some devices may require a reboot of their routing processors if this variable is changed. An agent which does not wish to reboot or modify its FRR mode MUST return an inconsistentValue error. Please consult the device's agent capability statement for more details."
cmplsFrrConstRowStatus	" This object is used to create, modify, and/or delete a row in this table."
cmplsFrrConstSetupPrio	" Indicates the setup priority of detour LSP." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001"
cmplsFrrDetourIncoming	" The number of detour LSPs entering the device if mplsFrrConstProtectionMethod is set to oneToOneBackup(0), or or 0 if mplsFrrConstProtectionMethod is set to facilityBackup(1)."
cmplsFrrDetourOriginating	" The number of detour LSPs originating at this PLR if mplsFrrConstProtectionMethod is set to oneToOneBackup(0). This object MUST return 0 if the mplsFrrConstProtectionMethod is set to facilityBackup(1)."
cmplsFrrDetourOutgoing	" The number of detour LSPs leaving the device if mplsFrrConstProtectionMethod is set to oneToOneBackup(0), or 0 if mplsFrrConstProtectionMethod is set to to facilityBackup(1)."
cmplsFrrFacRouteProtectedTunStatus	" Specifies the state of the protected tunnel. active This tunnel's label has been placed in the LFIB and is ready to be applied to incoming packets. ready - This tunnel's label entry has been created but is not yet in the LFIB. partial - This tunnel's label entry as not been fully created."
cmplsFrrFacRouteProtectingTunProtectionType	" Indicates type of the resource protection."
cmplsFrrFacRouteProtectingTunResvBw	" Specifies the amount of bandwidth in megabytes per second that is actually reserved by the backup tunnel for facility backup. This value is repeated here from the MPLS- TE MIB because the tunnel entry will reveal the bandwidth reserved by the signaling protocol, which is typically 0 for backup tunnels so as to not over-book bandwidth. However, internal reservations are typically made on the PLR, thus this value should be revealed here."
cmplsFrrLogEventDuration	" This object describes the duration of this event."
cmplsFrrLogEventReasonString	" This object contains an implementation-specific explanation of the event."
cmplsFrrLogEventTime	" This object provides the amount of time ticks since this event occured."
cmplsFrrLogEventType	" This object describes what type of fast reroute event occured."

cmplsFrrLogInterface	" This object indicates which interface was affected by this FRR event. This value may be set to 0 if mplsFrrConstProtectionMethod is set to oneToOneBackup(0)."
cmplsFrrLogTableCurrEntries	" Indicates the current number of entries in the FRR log table."
cmplsFrrLogTableMaxEntries	" Indicates the maximum number of entries allowed in the FRR Log table. Agents receiving SETs for values that cannot be used must return an inconsistent value error. If a manager sets this value to 0, this indicates that no logging should take place by the agent. If this value is returned as 0, this indicates that no additional log entries will be added to the current table either because the table has been completely filled or logging has been disabled. However, agents may wish to not delete existing entries in the log table so that managers may review them in the future. It is implied that when mplsFrrLogTableCurrEntries has reached the value of this variable, that logging entries may not continue to be added to the table, although existing ones may remain. Furthermore, an agent may begin to delete existing (perhaps the oldest entries) entries to make room for new ones."
cmplsFrrNotifMaxRate	" This variable indicates the number of milliseconds that must elapse between notification emissions. If events occur more rapidly, the implementation may simply fail to emit these notifications during that period, or may queue them until an appropriate time in the future. A value of 0 means no minimum elapsed period is specified."
cmplsFrrNotifsEnabled	" Enables or disables FRR notifications defined in this MIB module. Notifications are disabled by default."
cmplsFrrNumOfConfIfs	" Indicates the number of MPLS interfaces configured for protection by the FRR feature, otherwise this value MUST return 0 to indicate that LSPs traversing any interface may be protected."
cmplsFrrSwitchover	" The number of tunnel instances that are switched over to their corresponding detour LSP if mplsFrrConstProtectionMethod is set to oneToOneBackup(0), or tunnels being switched over if mplsFrrConstProtectionMethod is set to facilityBackup(1)."

CISCO-MPLS-TE-STD-EXT-MIB

This MIB module contains Cisco specific managed object definitions for MPLS Traffic Engineering (TE), not contained in MPLS-TE-STD-MIB.The auto bandwidth feature enables MPLS TE Tunnels to adapt automatically their bandwidth to their actual load."

The following table lists the tables associated with this MIB:

MIB Name	Description
cmplsTeLoadshareBalance	" This object indicates if the load-share balance is equal or unequal."
cmplsTeStdExtMIB	" This MIB module contains Cisco specific managed object definitions for MPLS Traffic Engineering (TE), not contained in MPLS-TE-STD-MIB. The auto bandwidth feature enables MPLS TE Tunnels to adapt automatically their bandwidth to their actual load."
cmplsTunnelAutoBWAdjThreshBW	" This object specifies the adjustment threshold bandwidth that needs to be overcome in order to trigger a new bandwidth application. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWAdjThreshPercs	" This object specifies the adjustment threshold percentage that needs to be overcome in order to trigger a new bandwidth application. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWApplicationFrequency	" This object specifies the bandwidth application period. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWApplications	" This object indicates the number of auto bandwidths applied. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWAppRejectReason	" This object indicates the reason for the bandwidth application rejection. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWCollectedSamples	" This object indicates the samples collected since the last auto-bandwidth application. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWCollectionFrequency	" This object specifies the sampling period for data rates. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."

cmplsTunnelAutoBWCollectOnlyRequested	" This object indicates the bandwidth that would have been requested by the auto-bandwidth algorithm if the auto-bandwidth functionality was enabled. If the collect only mode is enabled, the bandwidth change request will not be executed. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWHighest	" This object indicates the highest bandwidth sampled by the auto-bandwidth algorithm. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWJitter	" This object indicates the auto-bandwidth application jitter. Jitter is the extra time to be added to the application interval the first time the auto bandwidth is applied. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWLastApplicationTrigger	" This object indicates the trigger reason for the last bandwidth application. If mplsTunnelInstance is zero this object will be set to 'applicationNone'. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWLastAppliedBW	" This object indicates the last bandwidth applied by the auto-bandwidth algorithm. It will be set to zero if no bandwidth has been applied yet. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWMax	" This object specifies the maximum bandwidth that the auto-bandwidth algorithm can apply to a tunnel when the adjustment threshold is overcome. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWMin	" This object specifies the minimum bandwidth that the auto-bandwidth algorithm can apply to a tunnel when the adjustment threshold is overcome. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWOverflowApplications	" This object indicates the number of bandwidth applications due to overflow occurrences. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWOverflowLimit	" This object specifies the number of consecutive collections exceeding overflow threshold. If the application period has not completed when a cmplsTunnelAutoBWOverflowLimit overflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."

cmplsTunnelAutoBWOverflowOccurrences	" This object indicates the number of overflow occurrences since last application period. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWOverflowThreshBW	" This object specifies the adjustment threshold bandwidth that needs to be overcome in order to trigger an overflow occurrence. If the application period has not completed when a cmplsTunnelAutoBWOverflowLimit overflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWOverflowThreshPercs	" This object specifies the adjustment threshold percentage that needs to be overcome in order to trigger an overflow occurrence. If the application period has not completed when a cmplsTunnelAutoBWOverflowLimit overflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWRequested	" This object indicates the bandwidth requested by the auto-bandwidth algorithm. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWSignaled	" This object indicates the bandwidth signaled by the auto-bandwidth algorithm. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWStatus	" This object indicates the operational status [or mode] of the auto bandwidth algorithm: - autoBWDisabled: The auto-bandwidth algorithm is not running; - autoBWEnabled: The auto-bandwidth algorithm is running; - autoBWCollectOnlyMode: The auto-bandwidth algorithm is running, but the bandwidth applications are disabled;"
cmplsTunnelAutoBWUnderflowApplications	" This object indicates the number of bandwidth applications due to underflow occurrences. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWUnderflowHighestBW	" This object indicates the highest sample collected during an underflow sequence. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWUnderflowLimit	" This object specifies the number of consecutive collections under the underflow threshold. If the application period has not completed when a cmplsTunnelAutoBWUnderflowLimit underflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."

cmplsTunnelAutoBWUnderflowOccurrences	" This object indicates the number of underflow occurrences since last application period. If mplsTunnelInstance is zero this object will be set to zero. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWUnderflowThreshBW	" This object specifies the adjustment threshold bandwidth that needs to be overcome in order to trigger an underflow occurrence. If the application period has not completed when a cmplsTunnelAutoBWUnderflowLimit underflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelAutoBWUnderflowThreshPercs	" This object specifies the adjustment threshold percentage that needs to be overcome in order to trigger an underflow occurrence. If the application period has not completed when a cmplsTunnelAutoBWUnderflowLimit underflow has occurred, a new bandwidth will be applied. This object value is not aplicable if cmplsTunnelAutoBWStatus is 'autoBWDisabled'."
cmplsTunnelLoadShare	" This object indicates the Load-share as defined by the bandwidth attribute (default) or explicitly configured using the load-share command under tunnel configuration."

CISCO-NTP-MIB

This MIB module defines a MIB which provides mechanisms to monitor an NTP server.

The following table lists the tables associated with this MIB:

MIB Name	Description
cntpSysSrvStatus	" Current state of the NTP server with values coded as follows: 1: server status is unknown 2: server is not running 3: server is not synchronized to any time source 4: server is synchronized to its own local clock 5: server is synchronized to a local hardware refclock (e.g. GPS) 6: server is synchronized to a remote NTP server"

CISCO-PROCESS-MIB

The MIB module to describe active system processes.

The following table lists the tables associated with this MIB:

MIB Name	Description
cpmCPUTotal1minRev	" The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100)."
cpmCPUTotal5minRev	" The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100)."
cpmCPUTotalPhysicalIndex	" The entPhysicalIndex of the physical entity for which the CPU statistics in this entry are maintained. The physical entity can be a CPU chip, a group of CPUs, a CPU card etc. The exact type of this entity is described by its entPhysicalVendorType value. If the CPU statistics in this entry correspond to more than one physical entity (or to no physical entity), or if the entPhysicalTable is not supported on the SNMP agent, the value of this object must be zero."
cpmProcessAverageUSecs	" Average elapsed CPU time in microseconds when the process was active. This object deprecates the object cpmProcessuSecs."
cpmProcessName	" The name associated with this process. If the name is longer than 32 characters, it will be truncated to the first 31 characters, and a `*' will be appended as the last character to imply this is a truncated process name."
cpmProcessPID	" This object contains the process ID. cpmTimeCreated should be checked against the last time it was polled, and if it has changed the PID has been reused and the entire entry should be polled again."
cpmProcessTimeCreated	" The time when the process was created. The process ID and the time when the process was created, uniquely identifies a process."
cpmProcExtInvokedRev	" The number of times since cpmTimeCreated that the process has been invoked. This object deprecates cpmProcExtInvoked."
cpmProcExtMemAllocatedRev	" The sum of all the dynamically allocated memory that this process has received from the system. This includes memory that may have been returned. The sum of freed memory is provided by cpmProcExtMemFreedRev. This object deprecates cpmProcExtMemAllocated."
cpmProcExtMemFreedRev	" The sum of all memory that this process has returned to the system. This object deprecates cpmProcExtMemFreed."
cpmProcExtPriorityRev	" The priority level at which the process is running. This object deprecates cpmProcExtPriority."
cpmProcExtRuntimeRev	" The amount of CPU time the process has used, in microseconds. This object deprecates cpmProcExtRuntime."

cpmProcExtUtil1MinRev	" This object provides a general idea of how busy a process caused the processor to be over a 1 minute period. It is determined as a weighted decaying average of the current idle time over the longest idle time. Note that this information should be used as an estimate only. This object deprecates cpmProcExtUtil1Min and increases the value range to (0..100)."
cpmProcExtUtil5MinRev	" This object provides a general idea of how busy a process caused the processor to be over a 5 minute period. It is determined as a weighted decaying average of the current idle time over the longest idle time. Note that this information should be used as an estimate only. This object deprecates cpmProcExtUtil5Min and increases the value range to (0..100)."

CISCO-IETF-PW-MIB

This MIB contains managed object definitions for Pseudo Wire operation as in: Pate, P., et al, <draft-ietf-pwe3-framework>, Xiao, X., et al, <draft-ietf-pwe3-requirements>, Martini, L., et al, <draft-martini-l2circuit-trans-mpls>, and Martini, L., et al,<draft-martini-l2circuit-encap-mpls>.

The following table lists the tables associated with this MIB:

MIB Name	Description
cpwVcEntry	" A row in this table represents an emulated virtual connection (VC) across a packet network. It is indexed by cpwVcIndex, which uniquely identifying a singular connection. " INDEX { cpwVcIndex }
cpwVcHoldingPriority	" This object define the relative holding priority of the VC in a lowest-to-highest fashion, where 0 is the highest priority. VCs with the same priority are treated with equal priority. Dropped VC will be set 'dormant' (as indicated in cpwVcOperStatus). This value is significant if there are competing resources between VCs and the implementation support this feature. If not supported or not relevant, the value of zero MUST be used."
cpwVcID	" Used in the outgoing VC ID field within the 'Virtual Circuit FEC Element' when LDP signaling is used or PW ID AVP for L2TP." REFERENCE " Martini, et al, . and So, et al, . Note: as specified in l2circuit-trans: It is REQUIRED to assign the same VC ID, and VC type for a given circuit in both directions."
cpwVcIdMappingVcIndex	" The value that represent the VC in the cpwVcTable."

cpwVcInboundMode	" This object is used to enable greater security for implementation that use per platform VC label space. In strict mode, packets coming from the PSN are accepted only from tunnels that are associated to the same VC via the inbound tunnel table in the case of MPLS, or as identified by the source IP address in case of L2TP or IP PSN. The entries in the inbound tunnel table are either explicitly configured or implicitly known by the maintenance protocol used for VC set-up. If such association is not known, not configured or not desired, loose mode should be configured, and the node should accept the packet based on the VC label only regardless of the outer tunnel used to carry the VC."
cpwVcInboundOperStatus	" Indicates the actual operational status of this VC in the inbound direction. - down: if PW signaling has not yet finished, or indications available at the service level indicate that the VC is not passing packets. - testing: if AdminStatus at the VC level is set to test. - dormant: The VC is not available because of the required resources are occupied VC with higher priority VCs . - notPresent: Some component is missing to accomplish the set up of the VC. - lowerLayerDown: The underlying PSN is not in OperStatus 'up'. "
cpwVcInboundVcLabel	" The VC label used in the inbound direction (i.e. packets received from the PSN. It may be set up manually if owner is 'manual' or automatically otherwise. Examples: For MPLS PSN, it represents the 20 bits of VC tag, for L2TP it represent the 32 bits Session ID. If the label is not yet known (signaling in process), the object should return a value of 0xFFFF." REFERENCE " Martini, et al, Townsley, et al, "
cpwVcIndexNext	" This object contains an appropriate value to be used for cpwVcIndex when creating entries in the cpwVcTable. The value 0 indicates that no unassigned entries are available. To obtain the value of cpwVcIndex for a new entry in the cpwVcTable, the manager issues a management protocol retrieval operation to obtain the current value of cpwVcIndex. After each retrieval operation, the agent should modify the value to reflect the next unassigned index. After a manager retrieves a value the agent will determine through its local policy when this index value will be made available for reuse."
cpwVcLocalGroupID	" Used in the Group ID field sent to the peer PWES within the maintenance protocol used for VC setup, zero if not used." REFERENCE " Martini, et al, and So, et al, ."
cpwVcLocalIfMtu	" If not equal zero, the optional IfMtu object in the maintenance protocol will be sent with this value, representing the locally supported MTU size over the interface (or the virtual interface) associated with the VC." REFERENCE " Martini, et al, and So, et al, ."

cpwVcLocalIfString	" Each VC is associated to an interface (or a virtual interface) in the ifTable of the node as part of the service configuration. This object defines if the maintenance protocol will send the interface's name as appears on the ifTable in the name object as part of the maintenance protocol. If set to false, the optional element will not be sent." REFERENCE " Martini, et al, and So, et al, ."
cpwVcName	" The canonical name assigned to the VC."
cpwVcNotifRate	" This object defines the maximum number of PW VC notifications that can be emitted from the device per second."
cpwVcOperStatus	" Indicates the actual combined operational status of this VC. It is 'up' if both cpwVcInboundOperStatus and cpwVcOutboundOperStatus are in 'up' state. For all other values, if the VCs in both directions are of the same value it reflects that value, otherwise it is set to the most severe status out of the two statuses. The order of severance from most severe to less severe is: unknown, notPresent, down, lowerLayerDown, dormant, testing, up. The operator may consult the per direction OperStatus for fault isolation per direction."
cpwVcOutboundOperStatus	" Indicates the actual operational status of this VC in the outbound direction - down: if PW signaling has not yet finished, or indications available at the service level indicate that the VC is not passing packets. - testing: if AdminStatus at the VC level is set to test. - dormant: The VC is not available because of the required resources are occupied VC with higher priority VCs . - notPresent: Some component is missing to accomplish the set up of the VC. - lowerLayerDown: The underlying PSN is not in OperStatus 'up'. "
cpwVcOutboundVcLabel	" The VC label used in the outbound direction (i.e. toward the PSN). It may be set up manually if owner is 'manual' or automatically otherwise. Examples: For MPLS PSN, it represents the 20 bits of VC tag, for L2TP it represent the 32 bits Session ID. If the label is not yet known (signaling in process), the object should return a value of 0xFFFF." REFERENCE " Martini, et al, Townsley, et al, "
cpwVcOwner	" Set by the operator to indicate the protocol responsible for establishing this VC. Value 'manual' is used in all cases where no maintenance protocol (PW signaling) is used to set-up the VC, i.e. require configuration of entries in the VC tables including VC labels, etc. The value 'maintenanceProtocol' is used in case of standard signaling of the VC for the specific PSN, for example LDP for MPLS PSN as specified in or L2TP control protocol. Value 'other' is used for other types of signaling."
cpwVcPeerAddr	" This object contains the value of of the peer node address of the PW/PE maintenance protocol entity. This object should contain a value of 0 if not relevant (manual configuration of the VC)."

cpwVcPeerAddrType	" Denotes the address type of the peer node maintenance protocol (signaling) address if PW maintenance protocol is used for the VC creation. It should be set to 'unknown' if PE/PW maintenance protocol is not used, i.e. cpwVcOwner is set to 'manual'. "
cpwVcPeerMappingVcIndex	" The value that represent the VC in the cpwVcTable."
cpwVcPerfTotalDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this row Counter32 or Counter64 suffered a discontinuity. If no such discontinuities have occurred since the last re- initialization of the local management subsystem, then this object contains a zero value."
cpwVcPerfTotalErrorPackets	" Counter for number of error at VC level processing, for example packets received with unknown VC label."
cpwVcPerfTotalInHCBytes	" High capacity counter for number of bytes received by the VC (from the PSN)."
cpwVcPerfTotalInHCPackets	" High capacity counter for number of packets received by the VC (from the PSN)."
cpwVcPerfTotalOutHCBytes	" High capacity counter for number of bytes forwarded by the VC (to the PSN)."
cpwVcPerfTotalOutHCPackets	" High capacity counter for number of packets forwarded by the VC (to the PSN)."
cpwVcPsnType	" Set by the operator to indicate the PSN type on which this VC will be carried. Based on this object, the relevant PSN table entries are created in the in the PSN specific MIB modules. For example, if mpls(1) is defined, the agent create an entry in cpwVcMplsTable, which further define the MPLS PSN configuration. Note: the exact set of PSN types is yet to be worked out by the WG. "
cpwVcRemoteControlWord	" If maintenance protocol is used for VC establishment, this parameter indicates the received status of the control word usage, i.e. if packets will be received with control word or not. The value of 'notYetKnown' is used while the maintenance protocol has not yet received the indication from the remote node. In manual configuration of the VC this parameters indicate to the local node what is the expected encapsulation for the received packets. " REFERENCE " Martini, et al, and So, et al, ."
cpwVcRemoteGroupID	" Obtained from the Group ID field as received via the maintenance protocol used for VC setup, zero if not used. Value of 0xFFFF shall be used if the object is yet to be defined by the VC maintenance protocol." REFERENCE " Martini, et al, and So, et al, ."
cpwVcRemoteIfMtu	" The remote interface MTU as (optionally) received from the remote node via the maintenance protocol. Should be zero if this parameter is not available or not used." REFERENCE " Martini, et al, and So, et al, ."

cpwVcRemoteIfString	" Indicate the interface description string as received by the maintenance protocol, MUST be NULL string if not applicable or not known yet." REFERENCE " Martini, et al, and So, et al, ."
cpwVcRowStatus	" For creating, modifying, and deleting this row."
cpwVcSetUpPriority	" This object define the relative set-up priority of the VC in a lowest-to-highest fashion, where 0 is the highest priority. VCs with the same priority are treated with equal priority. Dropped VC will be set 'dormant' (as indicated in cpwVcOperStatus). This value is significant if there are competing resources between VCs and the implementation support this feature. If not supported or not relevant, the value of zero MUST be used."
cpwVcStorageType	" This variable indicates the storage type for this object."
cpwVcTimeElapsed	" The number of seconds, including partial seconds, that have elapsed since the beginning of the current measurement period. If, for some reason, such as an adjustment in the system's time-of-day clock, the current interval exceeds the maximum value, the agent will return the maximum value."
cpwVcType	" This value indicate the service to be carried over this VC. Note: the exact set of VC types is yet to be worked out by the WG. "
cpwVcUpDownNotifEnable	" If this object is set to true(1), then it enables the emission of cpwVcUp and cpwVcDown notifications; otherwise these notifications are not emitted." REFERENCE " See also RFC3413 for explanation that notifications are under the ultimate control of the MIB modules in this document."
cpwVcUpTime	" Number of consecutive ticks this VC has been 'up' in both directions together (i.e. 'up' is observed in cpwVcOperStatus.)"
cpwVcValidIntervals	" The number of previous 15-minute intervals for which data was collected. An agent with PW capability must be capable of supporting at least n intervals. The minimum value of n is 4, The default of n is 32 and the maximum value of n is 96. The value will be unless the measurement was (re-) started within the last (*15) minutes, in which case the value will be the number of complete 15 minute intervals for which the agent has at least some data. In certain cases (e.g., in the case where the agent is a proxy) it is possible that some intervals are unavailable. In this case, this interval is the maximum interval number for which data is available. "
cpwVcAdminStatus	" The desired operational status of this VC."
cpwVcControlWord	" Define if the control word will be sent with each packet by the local node." REFERENCE " Martini, et al, "
cpwVcCreateTime	" System time when this VC was created."
cpwVcDescr	" A textual string containing information about the VC. If there is no description this object contains a zero length string."

CISCO-IETF-PW-ENET-MIB

This MIB describes a model for managing Ethernet point-to-point pseudo wire services over a Packet Switched Network (PSN)."

The following table lists the tables associated with this MIB:

MIB Name	Description
cpwVcEnetPortIfIndex	" This object is used to specify the ifIndex of the ETHERNET port associated with this VC for point-to-point Ethernet service, or the ifIndex of the virtual interface of the VPLS instance associated with the PW if the service is VPLS. Two rows in this table can point to the same ifIndex only if: 1) It is required to support multiple COS on a MPLS PSN for the same service (i.e.: a combination of ports and VLANs) by the use of multiple VC, each with a different COS. 2) There is no overlap of VLAN values specified in cpwVcEnetPortVlan that are associated with this port. A value of zero indicate that association to an ifIndex is not yet known."
cpwVcEnetPortVlan	" This object define the VLAN value on the physical port (or VPLS virtual port) if a change is required to the VLAN value between the VC and the physical/virtual port. The value of this object can be ignored if the whole traffic from the port is forwarded to one VC independent of the tagging on the port, but it is RECOMENDED that the value in this case will be '4097' indicating not relevant. It MUST be equal to cpwVcEnetPwVlan if 'noChange' mode is used. The value 4096 indicate that no VLAN (i.e. untagged frames) on the port are associated to this VC. This allows the same behaviors as assigning 'Default VLAN' to un-tagged frames. "
cpwVcEnetRowStatus	" Enable creating, deleting and modifying this row." -- TBD: Need to specify exact interaction with other tables, and -- when rows can/cannot be created/deleted/modified.

cpwVcEnetStatsIllegalLength	" The number of packets that were received with an illegal Ethernet packet length on this VC. An illegal length is defined as being greater than the value in the advertised maximum MTU supported, or shorter than the allowed Ethernet packet size."
cpwVcEnetStatsIllegalVlan	" The number of packets received (from the PSN) on this VC with an illegal VLAN field, missing VLAN field that was expected, or A VLAN field when it was not expected. This counter is not relevant if the VC type is 'ethernet' (i.e. raw mode), and should be set to 0 by the agent to indicate this."
cpwVcEnetStorageType	" Indicates the storage type of this row."
cpwVcEnetVcIfIndex	" It is sometimes convenient to model the VC PW as a virtual interface in the ifTable. In these cases this object hold the value of the ifIndex in the ifTable representing this VC PW. A value of zero indicate no such association or association is not yet known."
cpwVcEnetVlanMode	" Indicate the mode of VLAN handling between the port associated to the VC and the VC encapsulation itself. - 'other' indicate operation that is not defined by this MIB. - 'portBased' indicates that the forwarder will forward packets between the port and the PW independent of their structure. - 'noChange' indicates that the VC contains the original user VLAN, as specified in cpwVcEnetPortVlan. - 'changeVlan' indicates that the VLAN field on the VC may be different than the VLAN field on the user's port. - 'removeVlan' indicates that the encapsulation on the VC does not include the original VLAN field. Note that PRI bits transparency is lost in this case. - 'addVlan' indicate that a VLAN field will be added on the PSN bound direction. cpwVcEnetPwVlan indicate the value that will be added. - 'removeVlan', 'addVlan' and 'changeVlan' implementation is not required. "

CISCO-IETF-PW-MPLS-MIB

This MIB complements the CISCO-IETF-PW-MIB for PW operation over MPLS.

The following table lists the tables associated with this MIB:

MIB Name	Description
cpwVcMplsExpBits	" Set by the operator to indicate the MPLS EXP bits to be used on the VC shim label if

	cpwVcMplsExpBitsMode is specifiedValue(2), zero otherwise."
cpwVcMplsExpBitsMode	" Set by the operator to indicate the way the VC shim label EXP bits are to be determined. The value of outerTunnel(1) is used where there is an outer tunnel - cpwVcMplsMplsType is mplsTe or mplsNonTe. Note that in this case there is no need to mark the VC label with the EXP bits since the VC label is not visible to the intermediate nodes. If there is no outer tunnel, specifiedValue(2) indicate that the value is specified by cpwVcMplsExpBits, and serviceDependant(3) indicate that the EXP bits are setup based on a rule specified in the emulated service specific tables, for example when the EXP bits are a function of 802.1p marking for Ethernet emulated service." REFERENCE " martini et al, "
cpwVcMplsLocalLdpEntityID	" The local LDP Entity index of the LDP entity to be used for this VC on the local node. Should be set to all zeros if not used." REFERENCE " "
cpwVcMplsLocalLdpID	" The local LDP identifier of the LDP entity creating this VC in the local node. As the VC labels are always set from the per platform label space, the last two octets in the LDP ID MUST be always both zeros." REFERENCE " , . "
cpwVcMplsMplsType	" Set by the operator to indicate the outer tunnel types, if exists. mplsTe is used if the outer tunnel was set-up by MPLS-TE, and mplsNonTe is used the outer tunnel was set up by LDP or manually. Combination of mplsTe and mplsNonTe may exist in case of outer tunnel protection. vcOnly is used if there is no outer tunnel label. vcOnly cannot be combined with mplsNonTe or mplsTe."
cpwVcMplsPeerLdpID	" The peer LDP identifier as identified from the LDP session. Should be zero if not relevant or not known yet." REFERENCE " , . "
cpwVcMplsStorageType	" This variable indicates the storage type for this row."
cpwVcMplsTtl	" Set by the operator to indicate the VC TTL bits to be used on the VC shim label." REFERENCE " martini et al, "

CISCO-RF-MIB

This MIB provides configuration control and status for the Redundancy Framework (RF) subsystem. RF provides a mechanism for logical redundancy of software functionality and is designed to support 1:1 redundancy on processor cards. RF is not intended to solve all redundancy schemes. Nor is RF designed to support redundant hardware, such as power supplies.

The following table lists the tables associated with this MIB:

MIB Name	Description
cRFCfgRedundancyMode	" Indicates the redundancy mode configured on the device."
cRFCfgRedundancyModeDescr	" Further clarifies or describes the redundancy mode indicated by cRFCfgRedundancyMode. Implementation-specific terminology associated with the current redundancy mode may be presented here."
cRFCfgRedundancyOperMode	" Indicate the operational redundancy mode of the device."
cRFStatusDuplexMode	" Indicates whether the redundant peer unit has been detected or not. If the redundant peer unit is detected, this object is true. If the redundant peer unit is not detected, this object is false."
cRFStatusFailoverTime	" The value of sysUpTime when the primary redundant unit took over as active. The value of this object will be 0 till the first switchover."
cRFStatusLastSwactReasonCode	" The reason for the last switch of activity."
cRFStatusManualSwactInhibit	" Indicates whether a manual switch of activity is permitted. If a manual switch of activity is allowed, this object is false. If a manual switch of activity is not allowed, this object is true. Note that the value of this object is the inverse of the status of manual SWACTs. This object does not indicate whether a switch of activity is or has occurred. This object only indicates if the user-controllable capability is enabled or not. A switch of activity is the event in which the standby redundant unit becomes active and the previously active unit becomes standby."
cRFStatusPeerStandByEntryTime	" The value of sysUpTime when the peer redundant unit entered the standbyHot state. The value will be 0 on system initialization."
cRFStatusPeerUnitId	" A unique identifier for the redundant peer unit. This identifier is implementation-specific but the method for selecting the id must remain consistent throughout the redundant system. Some example identifiers include: slot id, physical or logical entity id, or a unique id assigned internally by the RF subsystem."
cRFStatusPeerUnitState	" The current state of RF on the peer unit."

cRFStatusPrimaryMode	" Indicates whether this is the primary redundant unit or not. If this unit is the primary unit, this object is true. If this unit is the secondary unit, this object is false. Note that the terms 'primary/secondary' are not synonymous with the terms 'active/standby'. At any given time, the primary unit may be the active unit, or the primary unit may be the standby unit. Likewise, the secondary unit, at any given time, may be the active unit, or the secondary unit may be the standby unit. The primary unit is given a higher priority or precedence over the secondary unit. In a race condition (usually at initialization time) or any situation where the redundant units are unable to successfully negotiate activity between themselves, the primary unit will always become the active unit and the secondary unit will fall back to standby. Only one redundant unit can be the primary unit at any given time. The algorithm for determining the primary unit is system dependent, such as 'the redundant unit with the lower numeric unit id is always the primary unit.'"
cRFStatusRFClientDescr	" The description of the client which has registered with the Redundancy Facility."
cRFStatusRFClientRedTime	" Time taken for this client to become Redundant. This value is meaningful when the value of cRFStatusRFClientStatus is not 'noStatus'."
cRFStatusRFClientSeq	" The sequence number of the client. The system assigns the sequence numbers based on the order of registration of the Redundancy Facility clients. This is used for deciding order of RF events sent to clients."
cRFStatusRFClientStatus	" This object provides the status of the Redundancy Facility client."
cRFStatusRFModeCapsModeDescr	" The description of the device implementation specific terminology associated with its supported redundancy mode."
cRFStatusUnitId	" A unique identifier for this redundant unit. This identifier is implementation-specific but the method for selecting the id must remain consistent throughout the redundant system. Some example identifiers include: slot id, physical or logical entity id, or a unique id assigned internally by the RF subsystem."
cRFStatusUnitState	" The current state of RF on this unit."

CISCO-SONET-MIB

The MIB module to describe SONET/SDH interfaces objects. This is an extension to the standard SONET MIB(RFC 2558).

The following table lists the tables associated with this MIB:

MIB Name	Description
csNotificationsEnabled	" This object controls if the generation of ciscoSonetSectionStatusChange, ciscoSonetLineStatusChange, ciscoSonetPathStatusChange and ciscoSonetVTStatusChange notifications is enabled. If the value of this object is 'true(1)', then all notifications in this MIB are enabled; otherwise they are disabled."

CISCO-SELECTIVE-VRF-DOWNLOAD-MIB

This MIB module defines objects describing selective VRF download. The selective VRF download feature makes a best effort to download only those prefixes and labels to a physical entity required to forward traffic through the physical entity. The feature accomplishes this by characterizing roles for physical entities baed on their configuration.

The following table lists the tables associated with this MIB:

MIB Name	Description
csvdAdminEnable	" This object specifies the desired state of selective VRF download feature. When a managed system initializes, it starts with csvdAdminEnable in the true(1) state. As a result of either explicit management action or per configuration information retained by the managed system, csvdAdminEnable is then changed to false(2) state (or remains in the true(1) state."
csvdCounterDiscontinuityTime	" This object indicates the value of sysUpTime on the most recent occasion at which selective VRF download counters suffered a discontinuity. The relevant counters are the instances of any Counter32 objects contained in csvdStateTable. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
csvdEntityRoleChangeNotificationEnable	" This object specifies whether the system generates the csvdEntityRoleChangeNotification."
csvdOperEnable	" This object indicates the current operational state of selective VRF download feature. If csvdAdminEnable is changed then csvdOperEnable should change to the same value after the external action is triggered. As an external action implementations may require router reload or switchover of the route-processor for the change to take effect."

csvdRoleHistoryLastIndex	" This object indicates the value of csvdRoleHistoryIndex corresponding to the last row created in the csvdRoleHistoryTable."
csvdRoleHistorySize	" This object specifies the maximum number of rows the csvdRoleHistoryTable can contain at any given time. If the role changes and the csvdRoleHistoryTable already contains a number of rows equal to the value of this object, then it destroys the oldest row before creating a new one."

CISCO-SYSTEM-MIB

The systemGroup (see RFC 1907) provides a standard set of basic system information. This MIB module contains Cisco-defined extensions to the systemGroup."

The following table lists the tables associated with this MIB:

MIB Name	Description
csyClockDateAndTime	" The current local date and time for the system. Setting this object is equivalent to setting an automated clock and calendar. The value of the object will track the date and time from the value set. Note that due to hardware limitations some systems may not be able to preserve such meaning across reboots of the system, as indicated by csyClockLostOnReboot. A constant value of all zeros and length 8 indicates the system is not aware of the present date and time. This object may be read-only on some systems."
csyClockLostOnReboot	" Indication of whether the system can preserve knowledge of current date and time across a system reboot. A value of 'true' indicates the clock must be reset from some external source each time the system reboots. A value of 'false' indicates the system has the ability to keep time across reboots."
csyLocationCountry	" The country where the system is physically located. On some systems and for some technologies this value affects behavior, such as standards for communication. All such technologies should default to using the setting of this value, but may provide an override if necessary. The default value of this object is 'US'. Systems destined for other countries may use a different default. Systems in which the value does not affect operation should default to a zero-length value."
csyNotificationsEnable	" This object indicates whether the system produces the notifications defined by the ciscoSystemNotificationsGroup. A false value will prevent notifications from being generated by this system."

csyScheduledResetAction	" Writing reset(1) to this object perform the normal reset operation on the active supervisor module. Writing resetMinDown(2) to this object resets the system with the minimal system down time at the scheduled time. The resetMinDown(2) is only supported in systems with redundant supervisors."
csyScheduledResetReason	" Indicates the reason users input when issuing system's scheduled reset. After the system is reset, this object value will be empty octet string."
csyScheduledResetTime	" The scheduled date and time the switch will be reset at. The system will only take octet strings with length 8 for this object which indicates the local time of the switch. The maximum scheduled time is 24 days from the current system clock time. Setting this object value to be before the current system clock time or beyond the maximum scheduled time limit will be rejected by the system. Setting the object to all-zero octet strings will cancel the previously scheduled reset time and then the system will have no pending scheduled reset time. Setting this object value to be any valid octet strings other than the above cases will override the previously scheduled reset time and cause the system to be reset at the newly specified time. After the system has accepted the scheduled reset time, if the system clock is advanced ahead of the scheduled reset time, then reset will happen approximately 5 minutes after the current clock."
csySummerTimeStatus	" An indication of whether the summertime feature is enabled on this device. When this object is set to true, then csySummerTimeOffset, csySummerTimeRecurringStart and csySummerTimeRecurringEnd objects are set to default values provided by the system. When this object is set to false, then csySummerTimeOffset, csySummerTimeRecurringStart, csySummerTimeRecurringEnd objects are not instantiated and the summertime feature is disabled."

CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

Cisco VLAN ifTable Relationship MIB lists VLAN-id and ifIndex information for routed VLAN interfaces.

The following table lists the tables associated with this MIB:

MIB Name	Description
cviRoutedVlanIfIndex	" The index for the ifTable entry associated with this routed VLAN interface."

EtherLike-MIB

The MIB module to describe generic objects foR ethernet-like network interfaces.

The following table lists the tables associated with this MIB:

MIB Name	Description
dot3ControlFunctionsSupported	" A list of the possible MAC Control functions implemented for this interface." REFERENCE " [IEEE 802.3 Std.], 30.3.3.2, aMACControlFunctionsSupported."
dot3ControlInUnknownOpcodes	" A count of MAC Control frames received on this interface that contain an opcode that is not supported by this device. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCControlInUnknownOpcodes object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.3.5, aUnsupportedOpcodesReceived"
dot3HCControlInUnknownOpcodes	" A count of MAC Control frames received on this interface that contain an opcode that is not supported by this device. This counter is a 64 bit version of dot3ControlInUnknownOpcodes. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.3.5, aUnsupportedOpcodesReceived"
dot3HCInPauseFrames	" A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. This counter is a 64 bit version of dot3InPauseFrames. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.4.3, aPAUSEMACCtrlFramesReceived."

dot3HCOutPauseFrames	" A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. This counter is a 64 bit version of dot3OutPauseFrames. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.4.2, aPAUSEMACCtrlFramesTransmitted."
dot3HCStatsAlignmentErrors	" A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. This counter does not increment for group encoding schemes greater than 4 bits per group. This counter is a 64 bit version of dot3StatsAlignmentErrors. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.7, aAlignmentErrors"
dot3HCStatsFCSErrors	" A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Note: Coding errors detected by the physical layer for speeds above 10 Mb/s will cause the frame to fail the FCS check. This counter is a 64 bit version of dot3StatsFCSErrors. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.6, aFrameCheckSequenceErrors."

dot3HCStatsFrameTooLongs	" A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. This counter is a 64 bit version of dot3StatsFrameTooLongs. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.25, aFrameTooLongErrors."
dot3HCStatsInternalMacReceiveErrors	" A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. This counter is a 64 bit version of dot3StatsInternalMacReceiveErrors. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.15, aFramesLostDueToIntMACRcvError."

dot3HCStatsInternalMacTransmitErrors	" A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted. This counter is a 64 bit version of dot3StatsInternalMacTransmitErrors. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE "[IEEE 802.3 Std.], 30.3.1.1.12, aFramesLostDueToIntMACXmitError."
dot3HCStatsSymbolErrors	" For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter is a 64 bit version of dot3StatsSymbolErrors. It should be used on interfaces operating at 10 Gb/s or faster. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE "[IEEE 802.3 Std.], 30.3.2.1.5, aSymbolErrorDuringCarrier."

dot3InPauseFrames	"A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCInPauseFrames object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE "[IEEE 802.3 Std.], 30.3.4.3, aPAUSEMACCtrlFramesReceived."
dot3OutPauseFrames	"A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCOutPauseFrames object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE "[IEEE 802.3 Std.], 30.3.4.2, aPAUSEMACCtrlFramesTransmitted."
dot3PauseAdminMode	"This object is used to configure the default administrative PAUSE mode for this interface. This object represents the administratively-configured PAUSE mode for this interface. If auto-negotiation is not enabled or is not implemented for the active MAU attached to this interface, the value of this object determines the operational PAUSE mode of the interface whenever it is operating in full-duplex mode. In this case, a set to this object will force the interface into the specified mode. If auto-negotiation is implemented and enabled for the MAU attached to this interface, the PAUSE mode for this interface is determined by auto-negotiation, and the value of this object denotes the mode to which the interface will automatically revert if/when auto-negotiation is later disabled. Note that when auto-negotiation is running, administrative control of the PAUSE mode may be accomplished using the ifMauAutoNegCapAdvertisedBits object in the MAU-MIB. Note that the value of this object is ignored when the interface is not operating in full-duplex mode. An attempt to set this object to 'enabledXmit(2)' or 'enabledRcv(3)' will fail on

	interfaces that do not support operation at greater than 100 Mb/s."
dot3PauseOperMode	" This object reflects the PAUSE mode currently in use on this interface, as determined by either (1) the result of the auto-negotiation function or (2) if auto-negotiation is not enabled or is not implemented for the active MAU attached to this interface, by the value of dot3PauseAdminMode. Interfaces operating at 100 Mb/s or less will never return 'enabledXmit(2)' or 'enabledRcv(3)'. Interfaces operating in half-duplex mode will always return 'disabled(1)'. Interfaces on which auto-negotiation is enabled but not yet completed should return the value 'disabled(1)'."

dot3StatsAlignmentErrors	" A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check. The count represented by an instance of this object is incremented when the alignmentError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. This counter does not increment for group encoding schemes greater than 4 bits per group. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsAlignmentErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.7, aAlignmentErrors"
dot3StatsCarrierSenseErrors	" The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. The count represented by an instance of this object is incremented at most once per transmission attempt, even if the carrier sense condition fluctuates during a transmission attempt. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.13, aCarrierSenseErrors."
dot3StatsDeferredTransmissions	" A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy. The count represented by an instance of this object does not include frames involved in collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.9, aFramesWithDeferredXmissions."

dot3StatsDuplexStatus	" The current mode of operation of the MAC entity. 'unknown' indicates that the current duplex mode could not be determined. Management control of the duplex mode is accomplished through the MAU MIB. When an interface does not support autonegotiation, or when autonegotiation is not enabled, the duplex mode is controlled using ifMauDefaultType. When autonegotiation is supported and enabled, duplex mode is controlled using ifMauAutoNegAdvertisedBits. In either case, the currently operating duplex mode is reflected both in this object and in ifMauType. Note that this object provides redundant information with ifMauType. Normally, redundant objects are discouraged. However, in this instance, it allows a management application to determine the duplex status of an interface without having to know every possible value of ifMauType. This was felt to be sufficiently valuable to justify the redundancy." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.32, aDuplexStatus."
dot3StatsExcessiveCollisions	" A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.11, aFramesAbortedDueToXSColls."
dot3StatsFCSErrors	" A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error. The count represented by an instance of this object is incremented when the frameCheckError status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. Note: Coding errors detected by the physical layer for speeds above 10 Mb/s will cause the frame to fail the FCS check. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsFCSErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.6, aFrameCheckSequenceErrors."

dot3StatsFrameTooLongs	" A count of frames received on a particular interface that exceed the maximum permitted frame size. The count represented by an instance of this object is incremented when the frameTooLong status is returned by the MAC service to the LLC (or other MAC user). Received frames for which multiple error conditions pertain are, according to the conventions of IEEE 802.3 Layer Management, counted exclusively according to the error status presented to the LLC. For interfaces operating at 10 Gb/s, this counter can roll over in less than 80 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsFrameTooLongs object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.25, aFrameTooLongErrors."
dot3StatsIndex	" An index value that uniquely identifies an interface to an ethernet-like medium. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex." REFERENCE " RFC 2863, ifIndex"
dot3StatsInternalMacReceiveErrors	" A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsFrameTooLongs object, the dot3StatsAlignmentErrors object, or the dot3StatsFCSErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of receive errors on a particular interface that are not otherwise counted. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsInternalMacReceiveErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.15, aFramesLostDueToIntMACRcvError."

dot3StatsInternalMacTransmitErrors	" A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame is only counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object. The precise meaning of the count represented by an instance of this object is implementation- specific. In particular, an instance of this object may represent a count of transmission errors on a particular interface that are not otherwise counted. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsInternalMacTransmitErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.12, aFramesLostDueToIntMACXmitError."
dot3StatsLateCollisions	" The number of times that a collision is detected on a particular interface later than one slotTime into the transmission of a packet. A (late) collision included in a count represented by an instance of this object is also considered as a (generic) collision for purposes of other collision-related statistics. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.10, aLateCollisions."
dot3StatsMultipleCollisionFrames	" A count of frames that are involved in more than one collision and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsSingleCollisionFrames object. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.4, aMultipleCollisionFrames."

dot3StatsSingleCollisionFrames	" A count of frames that are involved in a single collision, and are subsequently transmitted successfully. A frame that is counted by an instance of this object is also counted by the corresponding instance of either the ifOutUcastPkts, ifOutMulticastPkts, or ifOutBroadcastPkts, and is not counted by the corresponding instance of the dot3StatsMultipleCollisionFrames object. This counter does not increment when the interface is operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.1.1.3, aSingleCollisionFrames."
dot3StatsSQETestErrors	" A count of times that the SQE TEST ERROR is received on a particular interface. The SQE TEST ERROR is set in accordance with the rules for verification of the SQE detection mechanism in the PLS Carrier Sense Function as described in IEEE Std. 802.3, 2000 Edition, section 7.2.4.6. This counter does not increment on interfaces operating at speeds greater than 10 Mb/s, or on interfaces operating in full-duplex mode. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 7.2.4.6, also 30.3.2.1.4, aSQETestErrors."

dot3StatsSymbolErrors	" For an interface operating at 100 Mb/s, the number of times there was an invalid data symbol when a valid carrier was present. For an interface operating in half-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than slotTime, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' or 'carrier extend error' on the GMII. For an interface operating in full-duplex mode at 1000 Mb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Data reception error' on the GMII. For an interface operating at 10 Gb/s, the number of times the receiving media is non-idle (a carrier event) for a period of time equal to or greater than minFrameSize, and during which there was at least one occurrence of an event that causes the PHY to indicate 'Receive Error' on the XGMII. The count represented by an instance of this object is incremented at most once per carrier event, even if multiple symbol errors occur during the carrier event. This count does not increment if a collision is present. This counter does not increment when the interface is operating at 10 Mb/s. For interfaces operating at 10 Gb/s, this counter can roll over in less than 5 minutes if it is incrementing at its maximum rate. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information, a management station is advised to poll the dot3HCStatsSymbolErrors object for 10 Gb/s or faster interfaces. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime." REFERENCE " [IEEE 802.3 Std.], 30.3.2.1.5, aSymbolErrorDuringCarrier."

ENTITY-MIB

The MIB module for representing multiple logical entities supported by a single SNMP agent.

The following table lists the tables associated with this MIB:

MIB Name	Description
entAliasMappingIdentifier	" The value of this object identifies a particular conceptual row associated with the indicated entPhysicalIndex and entLogicalIndex pair. Because only physical ports are modeled in this table, only entries that represent interfaces or ports are allowed. If an ifEntry exists on behalf of a particular physical port, then this object should identify the associated 'ifEntry'. For repeater ports, the appropriate row in the 'rptrPortGroupTable' should be identified instead. For example, suppose a physical port was represented by entPhysicalEntry.3, entLogicalEntry.15 existed for a repeater, and entLogicalEntry.22 existed for a bridge. Then there might be two related instances of entAliasMappingIdentifier: entAliasMappingIdentifier.3.15 == rptrPortGroupIndex.5.2 entAliasMappingIdentifier.3.22 == ifIndex.17 It is possible that other mappings (besides interfaces and repeater ports) may be defined in the future, as required. Bridge ports are identified by examining the Bridge MIB and appropriate ifEntries associated with each 'dot1dBasePort', and are thus not represented in this table."
entLastChangeTime	" The value of sysUpTime at the time a conceptual row is created, modified, or deleted in any of these tables: - entPhysicalTable - entLogicalTable - entLPMappingTable - entAliasMappingTable - entPhysicalContainsTable "
entLogicalDescr	" A textual description of the logical entity. This object should contain a string that identifies the manufacturer's name for the logical entity, and should be set to a distinct value for each version of the logical entity."
entLPPhysicalIndex	" The value of this object identifies the index value of a particular entPhysicalEntry associated with the indicated entLogicalEntity."
entPhysicalAlias	" This object is an 'alias' name for the physical entity, as specified by a network manager, and provides a non-volatile 'handle' for the physical entity. On the first instantiation of a physical entity, the value of entPhysicalAlias associated with that entity is set to the zero-length string. However, the agent may set the value to a locally unique default value, instead of a zero-length string. If write access is implemented for an instance of entPhysicalAlias, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAlias instance (associated with the same physical entity) for as long as that entity remains instantiated. This includes instantiations across all re-initializations/reboots of the network management system, including those resulting in a change of the physical entity's entPhysicalIndex value."

entPhysicalAssetID	" This object is a user-assigned asset tracking identifier (as specified by a network manager) for the physical entity, and provides non-volatile storage of this information. On the first instantiation of a physical entity, the value of entPhysicalAssetID associated with that entity is set to the zero-length string. Not every physical component will have an asset tracking identifier, or even need one. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to 'false(2)' (e.g., the repeater ports within a repeater module), do not need their own unique asset tracking identifier. An agent does not have to provide write access for such entities, and may instead return a zero-length string. If write access is implemented for an instance of entPhysicalAssetID, and a value is written into the instance, the agent must retain the supplied value in the entPhysicalAssetID instance (associated with the same physical entity) for as long as that entity remains instantiated. This includes instantiations across all re-initializations/reboots of the network management system, including those resulting in a change of the physical entity's entPhysicalIndex value. If no asset tracking information is associated with the physical component, then this object will contain a zero-length string."
entPhysicalChildIndex	" The value of entPhysicalIndex for the contained physical entity."
entPhysicalClass	" An indication of the general hardware type of the physical entity. An agent should set this object to the standard enumeration value that most accurately indicates the general class of the physical entity, or the primary class if there is more than one entity. If no appropriate standard registration identifier exists for this physical entity, then the value 'other(1)' is returned. If the value is unknown by this agent, then the value 'unknown(2)' is returned."
entPhysicalContainedIn	" The value of entPhysicalIndex for the physical entity which 'contains' this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of 'containment' relationships define a strict hierarchy; that is, recursion is not allowed. In the event that a physical entity is contained by more than one physical entity (e.g., double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex."
entPhysicalFirmwareRev	" The vendor-specific firmware revision string for the physical entity. Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific firmware programs are associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string."

entPhysicalIsFRU	" This object indicates whether or not this physical entity is considered a 'field replaceable unit' by the vendor. If this object contains the value 'true(1)' then this entPhysicalEntry identifies a field replaceable unit. For all entPhysicalEntries that represent components permanently contained within a field replaceable unit, the value 'false(2)' should be returned for this object."
entPhysicalParentRelPos	" An indication of the relative position of this 'child' component among all its 'sibling' components. Sibling components are defined as entPhysicalEntries that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects. An NMS can use this object to identify the relative ordering for all sibling components of a particular parent (identified by the entPhysicalContainedIn instance in each sibling entry). If possible, this value should match any external labeling of the physical component. For example, for a container (e.g., card slot) labeled as 'slot #3', entPhysicalParentRelPos should have the value '3'. Note that the entPhysicalEntry for the module plugged in slot 3 should have an entPhysicalParentRelPos value of '1'. If the physical position of this component does not match any external numbering or clearly visible ordering, then user documentation or other external reference material should be used to determine the parent-relative position. If this is not possible, then the agent should assign a consistent (but possibly arbitrary) ordering to a given set of 'sibling' components, perhaps based on internal representation of the components. If the agent cannot determine the parent-relative position for some reason, or if the associated value of entPhysicalContainedIn is '0', then the value '-1' is returned. Otherwise, a non-negative integer is returned, indicating the parent-relative position of this physical entity. Parent-relative ordering normally starts from '1' and continues to 'N', where 'N' represents the highest positioned child entity. However, if the physical entities (e.g., slots) are labeled from a starting position of zero, then the first sibling should be associated with an entPhysicalParentRelPos value of '0'. Note that this ordering may be sparse or dense, depending on agent implementation. The actual values returned are not globally meaningful, as each 'parent' component may use different numbering algorithms. The ordering is only meaningful among siblings of the same parent component. The agent should retain parent-relative position values across reboots, either through algorithmic assignment or use of non-volatile storage."

entPhysicalSoftwareRev	" The vendor-specific software revision string for the physical entity. Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software programs are associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string."
entPhysicalVendorType	" An indication of the vendor-specific hardware type of the physical entity. Note that this is different from the definition of MIB-II's sysObjectID. An agent should set this object to an enterprise-specific registration identifier value indicating the specific equipment type in detail. The associated instance of entPhysicalClass is used to indicate the general type of hardware device. If no vendor-specific registration identifier exists for this physical entity, or the value is unknown by this agent, then the value { 0 0 } is returned."

CISCO-ENTITY-SENSOR-MIB

The CISCO-ENTITY-SENSOR-MIB is used to monitor the values of sensors in the Entity-MIB (RFC 2037) entPhysicalTable.

The following table lists the tables associated with this MIB:

MIB Name	Description
entSensorMeasuredEntity	" This object identifies the physical entity for which the sensor is taking measurements. For example, for a sensor measuring the voltage output of a power-supply, this object would be the entPhysicalIndex of that power-supply; for a sensor measuring the temperature inside one chassis of a multi-chassis system, this object would be the enPhysicalIndex of that chassis. This object has a value of zero when the physical entity for which the sensor is taking measurements can not be represented by any one row in the entPhysicalTable, or that there is no such physical entity."
entSensorPrecision	" This variable indicates the number of decimal places of precision in fixed-point sensor values reported by entSensorValue. This variable is set to 0 when entSensorType is not a fixed-point type: e.g.'percentRH(9)', 'rpm(10)', 'cmm(11)', or 'truthvalue(12)'. This variable is set by the agent at start-up and the value does not change during operation."
entSensorScale	" This variable indicates the exponent to apply to sensor values reported by entSensorValue. This variable is set by the agent at start-up and the value does not change during operation."
entSensorStatus	" This variable indicates the present operational status of the sensor."

entSensorThresholdEvaluation	" This variable indicates the result of the most recent evaluation of the threshold. If the threshold condition is true, entSensorThresholdEvaluation is true(1). If the threshold condition is false, entSensorThresholdEvaluation is false(2). Thresholds are evaluated at the rate indicated by entSensorValueUpdateRate."
entSensorThresholdNotificationEnable	" This variable controls generation of entSensorThresholdNotification for this threshold. When this variable is 'true', generation of entSensorThresholdNotification is enabled for this threshold. When this variable is 'false', generation of entSensorThresholdNotification is disabled for this threshold."
entSensorThresholdRelation	" This variable indicates the relation between sensor value (entSensorValue) and threshold value (entSensorThresholdValue), required to trigger the alarm. when evaluating the relation, entSensorValue is on the left of entSensorThresholdRelation, entSensorThresholdValue is on the right. in pseudo-code, the evaluation-alarm mechanism is: ... if (entSensorStatus == ok) then if (evaluate(entSensorValue, entSensorThresholdRelation, entSensorThresholdValue)) then if (entSensorThresholdNotificationEnable == true)) then raise_alarm(sensor's entPhysicalIndex); endif endif endif ..."
entSensorThresholdSeverity	" This variable indicates the severity of this threshold."
entSensorThresholdValue	" This variable indicates the value of the threshold. To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision. However, you can directly compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."
entSensorType	" This variable indicates the type of data reported by the entSensorValue. This variable is set by the agent at start-up and the value does not change during operation."
entSensorValue	" This variable reports the most recent measurement seen by the sensor. To correctly display or interpret this variable's value, you must also know entSensorType, entSensorScale, and entSensorPrecision. However, you can compare entSensorValue with the threshold values given in entSensorThresholdTable without any semantic knowledge."
entSensorValueTimeStamp	" This variable indicates the age of the value reported by entSensorValue"
entSensorValueUpdateRate	" This variable indicates the rate that the agent updates entSensorValue."

ENTITY-STATE-MIB

This MIB defines a state extension to the Entity MIB

The following table lists the tables associated with this MIB:

MIB Name	Description
entStateAdmin	" The administrative state for this entity. This object refers to an entities administrative permission to service both other entities within its containment hierarchy as well other users of its services defined by means outside the scope of this MIB. Setting this object to 'notSupported' will result in an 'inconsistentValue' error. For entities that do not support administrative state, all set operations will result in an 'inconsistentValue' error. Some physical entities exhibit only a subset of the remaining administrative state values. Some entities cannot be locked, and hence this object exhibits only the 'unlocked' state. Other entities cannot be shutdown gracefully, and hence this object does not exhibit the 'shuttingDown' state. A value of 'inconsistentValue' will be returned if attempts are made to set this object to values not supported by its administrative model."
entStateAlarm	" The alarm status for this entity. It does not include the alarms raised on child components within its containment hierarchy. A value of 'unknown' means that this entity is unable to report alarm state. Note that this differs from 'indeterminate', which means that alarm state is supported and there are alarms against this entity, but the severity of some of the alarms is not known. If no bits are set, then this entity supports reporting of alarms, but there are currently no active alarms against this entity."
entStateLastChanged	" The value of this object is the date and time when the value of any of entStateAdmin, entStateOper, entStateUsage, entStateAlarm, or entStateStandby changed for this entity. If there has been no change since the last re-initialization of the local system, this object contains the date and time of local system initialization. If there has been no change since the entity was added to the local system, this object contains the date and time of the insertion."

entStateOper	" The operational state for this entity. Note that unlike the state model used within the Interfaces MIB [RFC2863], this object does not follow the administrative state. An administrative state of down does not predict an operational state of disabled. A value of 'testing' means that entity currently being tested and cannot therefore report whether it is operational or not. A value of 'disabled' means that an entity is totally inoperable and unable to provide service both to entities within its containment hierarchy, or to other receivers of its service as defined in ways outside the scope of this MIB. A value of 'enabled' means that an entity is fully or partially operable and able to provide service both to entities within its containment hierarchy, or to other receivers of its service as defined in ways outside the scope of this MIB. Note that some implementations may not be able to accurately report entStateOper while the entStateAdmin object has a value other than 'unlocked'. In these cases, this object MUST have a value of 'unknown'."
entStateStandby	" The standby status for this entity. Some entities will exhibit only a subset of the remaining standby state values. If this entity cannot operate in a standby role, the value of this object will always be 'providingService'."
entStateUsage	" The usage state for this entity. This object refers to an entity's ability to service more physical entities in a containment hierarchy. A value of 'idle' means this entity is able to contain other entities but that no other entity is currently contained within this entity. A value of 'active' means that at least one entity is contained within this entity, but that it could handle more. A value of 'busy' means that the entity is unable to handle any additional entities being contained in it. Some entities will exhibit only a subset of the usage state values. Entities that are unable to ever service any entities within a containment hierarchy will always have a usage state of 'busy'. Some entities will only ever be able to support one entity within its containment hierarchy and will therefore only exhibit values of 'idle' and 'busy'."

DISMAN-EXPRESSION-MIB

The MIB module for defining expressions of MIB objects for management purposes."

The following table lists the tables associated with this MIB:

MIB Name	Description
expResourceDeltaMinimum	" The minimum expExpressionDeltaInterval this system will accept. A system may use the larger values of this minimum to lessen the impact of constantly computing deltas. For larger delta sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all expressions created after it is set. The value -1 indicates that expResourceDeltaMinimum is irrelevant as the system will not accept 'deltaValue' as a value for expObjectSampleType. Unless explicitly resource limited, a system's value for this object should be 1, allowing as small as a 1 second interval for ongoing delta sampling. Changing this value will not invalidate an existing setting of expObjectSampleType."
expResourceDeltaWildcardInstanceMaximum	" For every instance of a deltaValue object, one dynamic instance entry is needed for holding the instance value from the previous sample, i.e. to maintain state. This object limits maximum number of dynamic instance entries this system will support for wildcarded delta objects in expressions. For a given delta expression, the number of dynamic instances is the number of values that meet all criteria to exist times the number of delta values in the expression. A value of 0 indicates no preset limit, that is, the limit is dynamic based on system operation and resources. Unless explicitly resource limited, a system's value for this object should be 0. Changing this value will not eliminate or inhibit existing delta wildcard instance objects but will prevent the creation of more such objects. An attempt to allocate beyond the limit results in expErrorCode being tooManyWildcardValues for that evaluation attempt."
expResourceDeltaWildcardInstanceResourceLacks	" The number of times this system could not evaluate an expression because that would have created a value instance in excess of expResourceDeltaWildcardInstanceMaximum."
expResourceDeltaWildcardInstances	" The number of currently active instance entries as defined for expResourceDeltaWildcardInstanceMaximum."
expResourceDeltaWildcardInstancesHigh	" The highest value of expResourceDeltaWildcardInstances that has

	occurred since initialization of the managed system."

IF-MIB

The MIB module to describe generic objects for network interface sub-layers. This MIB is an updated version of MIB-II's ifTable, and incorporates the extensions defined in RFC 1229."

The following table lists the tables associated with this MIB:

MIB Name	Description
ifAdminStatus	" The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state)."
ifAlias	" This object is an 'alias' name for the interface as specified by a network manager, and provides a non-volatile 'handle' for the interface. On the first instantiation of an interface, the value of ifAlias associated with that interface is the zero-length string. As and when a value is written into an instance of ifAlias through a network management set operation, then the agent must retain the supplied value in the ifAlias instance associated with the same interface for as long as that interface remains instantiated, including across all re-initializations/reboots of the network management system, including those which result in a change of the interface's ifIndex value. An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface. Some agents may support write-access only for interfaces having particular values of ifType. An agent which supports write access to this object is required to keep the value in non-volatile storage, but it may limit the length of new values depending on how much storage is already occupied by the current values for other interfaces."

ifConnectorPresent	" This object has the value 'true(1)' if the interface sublayer has a physical connector and the value 'false(2)' otherwise."
ifCounterDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity. The relevant counters are the specific instances associated with this interface of any Counter32 or Counter64 object contained in the ifTable or ifXTable. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
ifDescr	" A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software."
ifHCInBroadcastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCInMulticastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifInMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCInOctets	" The total number of octets received on the interface, including framing characters. This object is a 64-bit version of ifInOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCInUcastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCOutBroadcastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."

ifHCOutMulticastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCOutOctets	" The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHCOutUcastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifHighSpeed	" An estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If this object reports a value of `n' then the speed of the interface is somewhere in the range of `n-500,000' to `n+499,999'. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero."
ifInBroadcastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifIndex	" A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re- initialization."
ifInDiscards	" The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."

ifInErrors	" For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character- oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifInMulticastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifInOctets	" The total number of octets received on the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifInUcastPkts	" The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifInUnknownProtos	" For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifLastChange	" The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value."
ifLinkUpDownTrapEnable	" Indicates whether linkUp/linkDown traps should be generated for this interface. By default, this object should have the value enabled(1) for interfaces which do not operate on 'top' of any other interface (as defined in the ifStackTable), and disabled(2) otherwise."

ifMtu	" The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface."
ifName	" The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name, such as `le0' or a simple port number, such as `1', depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. Note that for an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string."
ifNumber	" The number of network interfaces (regardless of their current state) present on this system."
ifOperStatus	" The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."
ifOutBroadcastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifOutDiscards	" The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."

ifOutErrors	" For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifOutMulticastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifOutOctets	" The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifOutUcastPkts	" The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime."
ifPhysAddress	" The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length."
ifPromiscuousMode	" This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of true(1) when the station accepts all packets/frames transmitted on the media. The value true(1) is only legal on certain types of media. If legal, setting this object to a value of true(1) may require the interface to be reset before becoming effective. The value of ifPromiscuousMode does not affect the reception of broadcast and multicast packets/frames by the interface."
ifRcvAddressStatus	" This object is used to create and delete rows in the ifRcvAddressTable."

ifRcvAddressType	" This object has the value nonVolatile(3) for those entries in the table which are valid and will not be deleted by the next restart of the managed system. Entries having the value volatile(2) are valid and exist, but have not been saved, so that will not exist after the next restart of the managed system. Entries having the value other(1) are valid and exist but are not classified as to whether they will continue to exist after the next restart."
ifSpeed	" An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has no concept of bandwidth, this object should be zero."
ifStackLastChange	" The value of sysUpTime at the time of the last change of the (whole) interface stack. A change of the interface stack is defined to be any creation, deletion, or change in value of any instance of ifStackStatus. If the interface stack has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value."
ifStackStatus	" The status of the relationship between two sub-layers. Changing the value of this object from 'active' to 'notInService' or 'destroy' will likely have consequences up and down the interface stack. Thus, write access to this object is likely to be inappropriate for some types of interfaces, and many implementations will choose not to support write-access for any type of interface."
ifTableLastChange	" The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value."
ifType	" The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention."
ifXEntry	" An entry containing additional management information applicable to a particular interface." AUGMENTS { ifEntry }

IP-FORWARD-MIB

The MIB module for the management of CIDR multipath IP Routes.

The following table lists the tables associated with this MIB:

MIB Name	Description
ipCidrRouteAge	" The number of seconds since this route was last updated or otherwise determined to be correct. Note that no semantics of `too old' can be implied, except through knowledge of the routing protocol by which the route was learned."
ipCidrRouteDest	" The destination IP address of this route. This object may not take a Multicast (Class D) address value. Any assignment (implicit or otherwise) of an instance of this object to a value x must be rejected if the bitwise logical-AND of x with the value of the corresponding instance of the ipCidrRouteMask object is not equal to x."
ipCidrRouteIfIndex	" The ifIndex value that identifies the local interface through which the next hop of this route should be reached."
ipCidrRouteInfo	" A reference to MIB definitions specific to the particular routing protocol that is responsible for this route, as determined by the value specified in the route's ipCidrRouteProto value. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a syntactically valid object identifier, and any implementation conforming to ASN.1 and the Basic Encoding Rules must be able to generate and recognize this value."
ipCidrRouteMask	" Indicate the mask to be logical-ANDed with the destination address before being compared to the value in the ipCidrRouteDest field. For those systems that do not support arbitrary subnet masks, an agent constructs the value of the ipCidrRouteMask by reference to the IP Address Class. Any assignment (implicit or otherwise) of an instance of this object to a value x must be rejected if the bitwise logical-AND of x with the value of the corresponding instance of the ipCidrRouteDest object is not equal to ipCidrRouteDest."
ipCidrRouteMetric1	" The primary routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1."
ipCidrRouteMetric2	" An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1."
ipCidrRouteMetric3	" An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1."

ipCidrRouteMetric4	" An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1."
ipCidrRouteMetric5	" An alternate routing metric for this route. The semantics of this metric are determined by the routing- protocol specified in the route's ipCidrRouteProto value. If this metric is not used, its value should be set to -1."
ipCidrRouteNextHop	" On remote routes, the address of the next system en route; Otherwise, 0.0.0.0."
ipCidrRouteNextHopAS	" The Autonomous System Number of the Next Hop. The semantics of this object are determined by the routing- protocol specified in the route's ipCidrRouteProto value. When this object is unknown or not relevant, its value should be set to zero."
ipCidrRouteNumber	" The number of current ipCidrRouteTable entries that are not invalid. This object is deprecated in favor of inetCidrRouteNumber and the inetCidrRouteTable."
ipCidrRouteProto	" The routing mechanism via which this route was learned. Inclusion of values for gateway routing protocols is not intended to imply that hosts should support those protocols."
ipCidrRouteStatus	" The row status variable, used according to row installation and removal conventions."
ipCidrRouteTos	" The policy specifier is the IP TOS Field. The encoding of IP TOS is as specified by the following convention. Zero indicates the default path if no more specific policy applies
ipCidrRouteType	" The type of route. Note that local(3) refers to a route for which the next hop is the final destination; remote(4) refers to a route for which the next hop is not the final destination. Routes that do not result in traffic forwarding or rejection should not be displayed, even if the implementation keeps them stored internally. reject (2) refers to a route that, if matched, discards the message as unreachable. This is used in some protocols as a means of correctly aggregating routes."
inetCidrRouteDiscards	" The number of valid route entries discarded from the inetCidrRouteTable. Discarded route entries do not appear in the inetCidrRouteTable. One possible reason for discarding an entry would be to free-up buffer space for other route table entries."

inetCidrRouteNumber	" The number of current inetCidrRouteTable entries that are not invalid."

IP-MIB

The MIB module for managing IP and ICMP implementations, but excluding their management of IP routes.

The following table lists the tables associated with this MIB:

MIB Name	Description
Ip	
ipAddressCreated	" The value of sysUpTime at the time this entry was created. If this entry was created prior to the last re-initialization of the local network management subsystem, then this object contains a zero value."
ipAddressIfIndex	" The index value that uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB's ifIndex."
ipAddressLastChanged	" The value of sysUpTime at the time this entry was last updated. If this entry was updated prior to the last re- initialization of the local network management subsystem, then this object contains a zero value."
ipAddressOrigin	" The origin of the address."
ipAddressPrefix	" A pointer to the row in the prefix table to which this address belongs. May be { 0 0 } if there is no such row."
ipAddressPrefixAdvPreferredLifetime	" The remaining length of time, in seconds, that this prefix will continue to be preferred, i.e., time until deprecation. A value of 4,294,967,295 represents infinity. The address generated from a deprecated prefix should no longer be used as a source address in new communications, but packets received on such an interface are processed as expected. The default for IPv4 prefixes is 4,294,967,295 (infinity)." REFERENCE " For IPv6 RFC 2461, especially sections 2 and 4.6.2 and RFC 2462"
ipAddressPrefixAdvValidLifetime	" The remaining length of time, in seconds, that this prefix will continue to be valid, i.e., time until invalidation. A value of 4,294,967,295 represents infinity. The address generated from an invalidated prefix should not appear as the destination or source address of a packet. The default for IPv4 prefixes is 4,294,967,295 (infinity)." REFERENCE " For IPv6 RFC 2461, especially sections 2 and 4.6.2 and RFC 2462"

ipAddressPrefixAutonomousFlag	" Autonomous address configuration flag. When true(1), indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address). If false(2), it is not used to auto- configure a local interface address. The default for IPv4 prefixes is 'false(2)'." REFERENCE " For IPv6 RFC 2461, especially sections 2 and 4.6.2 and RFC 2462"
ipAddressPrefixOnLinkFlag	" This object has the value 'true(1)', if this prefix can be used for on-link determination; otherwise, the value is 'false(2)'. The default for IPv4 prefixes is 'true(1)'." REFERENCE " For IPv6 RFC 2461, especially sections 2 and 4.6.2 and RFC 2462"
ipAddressPrefixOrigin	" The origin of this prefix."
ipAddressRowStatus	" The status of this conceptual row. The RowStatus TC requires that this DESCRIPTION clause states under which circumstances other objects in this row can be modified. The value of this object has no effect on whether other objects in this conceptual row can be modified. A conceptual row can not be made active until the ipAddressIfIndex has been set to a valid index."
ipAddressStatus	" The status of the address, describing if the address can be used for communication. In the absence of other information, an IPv4 address is always preferred(1)."
ipAddressStorageType	" The storage type for this conceptual row. If this object has a value of 'permanent', then no other objects are required to be able to be modified."
ipAddressType	" The type of address. broadcast(3) is not a valid value for IPv6 addresses (RFC 3513)."
ipAdEntAddr	" The IPv4 address to which this entry's addressing information pertains."
ipAdEntBcastAddr	" The value of the least-significant bit in the IPv4 broadcast address used for sending datagrams on the (logical) interface associated with the IPv4 address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet and network broadcast addresses used by the entity on this (logical) interface."
ipAdEntIfIndex	" The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of the IF-MIB's ifIndex."
ipAdEntNetMask	" The subnet mask associated with the IPv4 address of this entry. The value of the mask is an IPv4 address with all the network bits set to 1 and all the hosts bits set to 0."
ipAdEntReasmMaxSize	" The size of the largest IPv4 datagram which this entity can re-assemble from incoming IPv4 fragmented datagrams received on this interface."

IPV6-MIB

The MIB module for entities implementing the IPv6 protocol."

The following table lists the tables associated with this MIB:

MIB Name	Description
ipv6DefaultHopLimit	" The default value inserted into the Hop Limit field of the IPv6 header of datagrams originated at this entity, whenever a Hop Limit value is not supplied by the transport layer protocol."
ipv6Forwarding	" The indication of whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a `wrongValue' response if a management station attempts to change this object to an inappropriate value."
ipv6Interfaces	" The number of IPv6 interfaces (regardless of their current state) present on this system."
ipv6IpForwarding	" The indication of whether this entity is acting as an IPv6 router on any interface in respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except those source-routed via the host). When this object is written, the entity SHOULD save the change to non-volatile storage and restore the object from non-volatile storage upon re-initialization of the system."

ISIS-MIB

This document describes a management information base for the IS-IS Routing protocol, as described in ISO 1058 when it is used to construct routing tables for IP networks, as described in RFC 1195

The following table lists the tables associated with this MIB:

MIB Name	Description
isisAreaAddr	" An area address reported in a Level 1 LSP."
isisCirc3WayEnabled	" Is this circuit enabled to run 3Way handshake?"
isisCircAdjChanges	" The number of times an adjacency state change has occurred on this circuit." REFERENCE "{ISIS.aoi changesInAdjacencyState (40)}"
isisCircAdminState	" The administrative state of the circuit."
isisCircAuthFails	" The number of times an IS-IS control PDU with the correct auth type has failed to pass authentication validation."
isisCircAuthTypeFails	" The number of times an IS-IS control PDU with an auth type field different from that for this system has been received."

isisCircExistState	" The existence state of this circuit. Setting the state to 'notInService' halts the generation and processing of IS-IS protocol PDUs on this circuit. Setting the state to destroy will also erase any configuration associated with the circuit. Support for 'createAndWait' and 'notInService' is not required. A row entry cannot be modified when the value of this object is 'active'."
isisCircExtDomain	" If true, suppress normal transmission of and interpretation of Intra-domain IS-IS PDUs on this circuit." REFERENCE "{ISIS.aoi externalDomain (46)}"
isisCircExtendedCircID	" The value to be used as the extended circuit ID in 3Way handshake. This value is only used if isisCirc3WayEnabled is true, and it must be unique across all circuits on this IS."
isisCircIDFieldLenMismatches	" The number of times an IS-IS control PDU with an ID field length different from that for this system has been received." REFERENCE "{ISIS.aoi iDFieldLengthMismatches (25)}"
isisCircIfIndex	" The value of ifIndex for the interface to which this circuit corresponds. This object cannot be modified after creation."
isisCircInitFails	" The number of times initialization of this circuit has failed. This counts events such as PPP NCP failures. Failures to form an adjacency are counted by isisCircRejAdjs."
isisCircLANDesISChanges	" The number of times the Designated IS has changed on this circuit at this level. If the circuit is point to point, this count is zero."
isisCircLastUpTime	" How long the circuit has been enabled, measured in hundredths of seconds since the last re-initialization of the network management subsystem; 0 if the circuit has never been 'on'."
isisCircLevelCSNPInterval	" Interval of time, in seconds, between periodic transmission of a complete set of CSNPs on multiaccess networks if this router is the designated router at this level. This object follows the ResettingTimer behavior." REFERENCE "{ISIS.aoi completeSNPInterval (8)}"
isisCircLevelDesIS	" The ID of the LAN-Designated Intermediate System on this circuit at this level. If, for any reason, this system is not partaking in the relevant Designated Intermediate System election process, then the value returned is the zero-length OCTET STRING." REFERENCE "{ISIS.aoi l2DesignatedIntermediateSystem (75)}"
isisCircLevelDRHelloTimer	" Period, in milliseconds, between Hello PDUs on multiaccess networks when this IS is the Designated Intermediate System. This object follows the ResettingTimer behavior." REFERENCE "{ISIS.aoi iSISHelloTimer (45)}"
isisCircLevelHelloMultiplier	" This value is multiplied by the corresponding HelloTimer, and the result in seconds (rounded up) is used as the holding time in transmitted hellos, to be used by receivers of hello packets from this IS." REFERENCE "{ISIS.aoi iSISHelloTimer (45)}"

isisCircLevelHelloTimer	" Maximum period, in milliseconds, between IIH PDUs on multiaccess networks at this level for LANs. The value at L1 is used as the period between Hellos on L1L2 point-to-point circuits. Setting this value at level 2 on an L1L2 point-to-point circuit will result in an error of InconsistentValue. This object follows the ResettingTimer behavior." REFERENCE " {ISIS.aoi iSISHelloTimer (45)}"
isisCircLevelID	" On a point-to-point circuit with a fully initialized adjacency to a peer IS, the value of this object is the circuit ID negotiated during adjacency initialization. On a point to point circuit without such an adjacency, the value is the concatenation of the local system ID and the one-byte isisCircLevelIDOctet for this circuit, i.e., the value that would be proposed for the circuit ID. On other circuit types, the value returned is the zero- length OCTET STRING." REFERENCE " {ISIS.aoi ptPtCircuitID (51)}"
isisCircLevelIDOctet	" A one-byte identifier for the circuit selected by the Intermediate System. On point-to-point circuits, the value is used as the Local Circuit ID in point-to-point IIH PDUs transmitted on this circuit. In this case, values of isisCircLevelIDOctet do not need to be unique. For broadcast circuits, the value is used to generate the LAN ID that will be used if this Intermediate System is elected as the Designated IS on this circuit. The value is required to differ on LANs where the Intermediate System is the Designated Intermediate System."
isisCircLevelISPriority	" The priority for becoming the LAN-Designated Intermediate System at this level." REFERENCE " {ISIS.aoi l2IntermediateSystemPriority (73)}"
isisCircLevelLSPThrottle	" Minimal interval of time, in milliseconds, between transmissions of LSPs on an interface at this level." REFERENCE " {ISIS.aoi minimumBroadcastLSPTransmissionInterval (5)}"
isisCircLevelMetric	" The metric value of this circuit for this level." REFERENCE " {ISIS.aoi l1DefaultMetric (35)}"
isisCircLevelMinLSPRetransInt	" Minimum interval, in seconds, between re-transmission of an LSP at this level. This object follows the ResettingTimer behavior. Note that isisCircLevelLSPThrottle controls how fast we send back-to-back LSPs. This variable controls how fast we re-send the same LSP." REFERENCE " {ISIS.aoi minimumLSPTransmissionInterval (5)}"
isisCircLevelPartSNPInterval	" Minimum interval, in seconds, between sending Partial Sequence Number PDUs at this level. This object follows the ResettingTimer behavior." REFERENCE " {ISIS.aoi partialSNPInterval (14)}"

isisCircLevelType	" Indicates which type of packets will be sent and accepted on this circuit. The values set will be saved, but the values used will be modified by the settings of isisSysLevelType. Thus, if the isisSysTpe is level2 and the isisCircLevelType for a circuit is level1, the circuit will not send or receive IS-IS packets. This object follows the ReplaceOnlyWhileDisabled behavior."
isisCircLevelWideMetric	" The wide metric value of this circuit for this level."
isisCircMaxAreaAddrMismatches	" The number of times an IS-IS control PDU with a max area address field different from that for this system has been received." REFERENCE "{ISIS.aoi iDFieldLengthMismatches (25)}"
isisCircMeshGroup	" Circuits in the same mesh group act as a virtual multiaccess network. LSPs seen on one circuit in a mesh group will not be flooded to another circuit in the same mesh group. If isisCircMeshGroupEnabled is inactive or blocked, this value is ignored." REFERENCE "{ RFC 2973 }"
isisCircMeshGroupEnabled	" Is this port a member of a mesh group, or is it blocked? Circuits in the same mesh group act as a virtual multiaccess network. LSPs seen on one circuit in a mesh group will not be flooded to another circuit in the same mesh group." REFERENCE "{ RFC 2973 }"
isisCircNumAdj	" The number of adjacencies on this circuit." REFERENCE "{ISIS.aoi changesInAdjacencyState (40)}"
isisCircPassiveCircuit	" Should we include this interface in LSPs, even if it is not running the IS-IS Protocol?"
isisCircRejAdjs	" The number of times an adjacency has been rejected on this circuit." REFERENCE "{ISIS.aoi rejectedAdjacencies (42)}"
isisCircSmallHellos	" Can we send unpadded hellos on LAN circuits? False means the LAN Hellos must be padded. Implementations should allow the administrator to read this value. An implementation need not be able to support unpadded hellos to be conformant."
isisCircType	" The type of the circuit. This object follows the ReplaceOnlyWhileDisabled behavior. The type specified must be compatible with the type of the interface defined by the value of isisCirclfIndex." REFERENCE "{ISIS.aoi type (33)}"
isisISAdj3WayState	" The 3Way state of the adjacency. These are picked to match the historical on-the-wire representation of the 3Way state and are not intended to match isisISAdjState." REFERENCE "{ RFC 3373 }"
isisISAdjAreaAddress	" One Area Address as reported in IIH PDUs received from the neighbor."
isisISAdjHoldTimer	" The holding time, in seconds, for this adjacency. This value is based on received IIH PDUs and the elapsed time since receipt." REFERENCE "{ISIS.aoi holdingTimer (85)}"

isisISAdjIPAddrAddress	" One IP Address as reported in IIH PDUs received from the neighbor. The type of this address is determined by the value of the isisISAdjIPAddrType object."
isisISAdjIPAddrType	" The type of one IP Address as reported in IIH PDUs received from the neighbor."
isisISAdjLastUpTime	" When the adjacency most recently entered the state 'up', measured in hundredths of a second since the last re-initialization of the network management subsystem. Holds 0 if the adjacency has never been in state 'up'."
isisISAdjNbrExtendedCircID	" The 4-byte Extended Circuit ID learned from the Neighbor during 3-way handshake, or 0."
isisISAdjNeighPriority	" Priority of the neighboring Intermediate System for becoming the Designated Intermediate System." REFERENCE " {ISIS.aoi IANPriority (86)}"
isisISAdjNeighSNPAAddress	" The SNPA address of the neighboring system." REFERENCE " {ISIS.aoi neighbourSNPAAddress (79)}"
isisISAdjNeighSysID	" The system ID of the neighboring Intermediate System." REFERENCE " {ISIS.aoi neighbourSystemIds (83)}"
isisISAdjNeighSysType	" The type of the neighboring system." REFERENCE " {ISIS.aoi neighbourSystemType (80)}"
isisISAdjProtSuppProtocol	" One supported protocol as reported in IIH PDUs received from the neighbor."
isisISAdjState	" The state of the adjacency." REFERENCE " {ISIS.aoi adjacencyState (78)}"
isisISAdjUsage	" How is the adjacency used? On a point-to-point link, this might be level1and2, but on a LAN, the usage will be level1 on the adjacency between peers at L1, and level2 for the adjacency between peers at L2." REFERENCE " {ISIS.aoi adjacencyUsage (82)}"
isisLSPAttributes	" Flags carried by the LSP."
isisLSPChecksum	" The 16-bit Fletcher Checksum for this LSP."
isisLSPLifetimeRemain	" The remaining lifetime, in seconds, for this LSP."
isisLSPPDULength	" The length of this LSP."
isisLSPSeq	" The sequence number for this LSP."
isisLSPTLVChecksum	" The 16-bit Fletcher Checksum for this LSP."
isisLSPTLVLen	" The length of this TLV."
isisLSPTLVSeq	" The sequence number for this LSP."
isisLSPTLVType	" The type of this TLV."
isisLSPTLVValue	" The value of this TLV."
isisLSPZeroLife	" Is this LSP being purged by this system?"

isisManAreaAddrExistState	" The state of the isisManAreaAddrEntry. If the isisSysAdminState for this Intermediate System is 'on' and an attempt is made to set this object to the value 'destroy' or 'notInService' when this is the only isisManAreaAddrEntry in state 'active' for this Intermediate System should return inconsistentValue. A row entry cannot be modified when the value of this object is 'active'."
isisPacketCountCSNP	" The number of IS-IS CSNPs seen in this direction at this level." REFERENCE " {ISIS.aoi iSISControlPDUsSent (43)}"
isisPacketCountESHello	" The number of ES Hello PDUs seen in this direction. ESH PDUs are counted at the lowest enabled level: at L1 on L1 or L1L2 circuits, and at L2 otherwise."
isisPacketCountIIHello	" The number of IS-IS Hello PDUs seen in this direction at this level. Point-to-Point IIH PDUs are counted at the lowest enabled level: at L1 on L1 or L1L2 circuits, and at L2 otherwise." REFERENCE " {ISIS.aoi iSISControlPDUsSent (43)}"
isisPacketCountISHello	" The number of ES-IS Hello PDUs seen in this direction. ISH PDUs are counted at the lowest enabled level: at L1 on L1 or L1L2 circuits, and at L2 otherwise."
isisPacketCountLSP	" The number of IS-IS LSPs seen in this direction at this level." REFERENCE " {ISIS.aoi iSISControlPDUsSent (43)}"
isisPacketCountPSNP	" The number of IS-IS PSNPs seen in this direction at this level." REFERENCE " {ISIS.aoi iSISControlPDUsSent (43)}"
isisPacketCountUnknown	" The number of unknown IS-IS PDUs seen at this level." REFERENCE " {ISIS.aoi iSISControlPDUsSent (43)}"
isisRouterHostName	" The hostname listed in the LSP, or a zero-length string if none."
isisRouterID	" The Router ID found in the LSP, or zero if none."
isisSysAdminState	" The administrative state of this Intermediate System. Setting this object to the value 'on' when its current value is 'off' enables the Intermediate System. Configured values MUST survive an agent reboot."
isisSysID	" The ID for this Intermediate System. This value is appended to each of the area addresses to form the Network Entity Titles. The derivation of a value for this object is implementation specific. Some implementations may automatically assign values and not permit an SNMP write, while others may require the value to be set manually. Configured values MUST survive an agent reboot." REFERENCE " {ISIS.aoi systemId (119)}"
isisSysL2toL1Leaking	" If true, allow the router to leak L2 routes into L1. Configured values MUST survive an agent reboot."
isisSysLevelMetricStyle	" Which style of metric do we generate in our LSPs at this level?"

isisSysLevelMinLSPGenInt	" Minimum interval, in seconds, between successive generation of LSPs with the same LSPID at this level by this Intermediate System." REFERENCE " {ISIS.aoi minimumLSPGenerationInterval (11)}"
isisSysLevelOrigLSPBuffSize	" The maximum size of LSPs and SNPs originated by this Intermediate System at this level. This object may not be modified when the isisSysAdminState variable is in state 'on' for this Intermediate System." REFERENCE " {ISIS.aoi originatingL1LSPBufferSize (9)}"
isisSysLevelSetOverload	" Administratively set the overload bit for the level. The overload bit MUST continue to be set if the implementation runs out of memory, independent of this variable. It may also be set manually independent of this variable, using the isisSysLevelSetOverloadUntil object."
isisSysLevelSetOverloadUntil	" If this object is non-zero, the overload bit is set at this level when the isisSysAdminState variable goes to state 'on' for this Intermediate System. The overload bit remains set for isisSysLevelSetOverloadUntil seconds. When isisSysLevelSetOverloadUntil seconds have elapsed, the overload flag remains set if the implementation has run out of memory, or if it is set manually using the isisSysLevelSetOverload object. If isisSysLevelSetOverload is false, the system clears the overload bit when isisSysLevelSetOverloadUntil seconds have elapsed, if the system has not run out of memory."
isisSysLevelSPFConsiders	" Which style of metric do we consider in our SPF computation at this level?"
isisSysLevelState	" The state of the database at this level. The value 'off' indicates that IS-IS is not active at this level. The value 'on' indicates that IS-IS is active at this level and is not overloaded. The value 'waiting' indicates a database that is low on an essential resource, such as memory. The administrator may force the state to 'overloaded' by setting the object isisSysLevelSetOverload. If the state is 'waiting' or 'overloaded', we originate LSPs with the overload bit set." REFERENCE " {ISIS.aoi l1State (17)}"
isisSysLevelTEEnabled	" Do we do Traffic Engineering at this level?"
isisSysLevelType	" At which levels is the Intermediate System running? This object may not be modified when the isisSysAdminState variable is in state 'on' for this Intermediate System. Configured values MUST survive an agent reboot." REFERENCE " {ISIS.aoi iSType (2)}"
isisSysMaxAge	" Value to place in RemainingLifeTime field of the LSPs we generate. This should be at least 300 seconds greater than isisSysMaxLSPGenInt. Configured values MUST survive an agent reboot."

isisSysMaxLSPGenInt	" Maximum interval, in seconds, between generated LSPs by this Intermediate System. This object follows the ResettingTimer behavior. The value must be greater than any value configured for isisSysLevelMinLSPGenInt, and should be at least 300 seconds less than isisSysMaxAge. Configured values MUST survive an agent reboot." REFERENCE "{ISIS.aoi maximumLSPGenerationInterval (6)}"
isisSysMaxPathSplits	" Maximum number of paths with equal routing metric value which it is permitted to split between. This object may not be modified when the isisSysAdminState variable is in state 'on' for this Intermediate System. Configured values MUST survive an agent reboot." REFERENCE "{ISIS.aoi maximumPathSplits (3)}"
isisSysNotificationEnable	" If this object is set to true(1), then it enables the emission of IS-IS Notifications. If it is set to false(2), these notifications are not sent. Configured values MUST survive an agent reboot."
isisSysPollESHelloRate	" The value, in seconds, to be used for the suggested ES configuration timer in ISH PDUs when soliciting the ES configuration. Configured values MUST survive an agent reboot." REFERENCE "{ISIS.aoi pollESHelloRate (13)}"
isisSysProtSupported	" This attribute contains the set of protocols supported by this Intermediate System."
isisSysReceiveLSPBufferSize	" Size of the largest buffer we are designed or configured to store. This should be at least as big as the maximum isisSysLevelOrigLSPBuffSize supported by the system. If resources allow, we will store and flood LSPs larger than isisSysReceiveLSPBufferSize, as this can help avoid problems in networks with different values for isisSysLevelOrigLSPBuffSize. Configured values MUST survive an agent reboot."
isisSysStatAttmptToExMaxSeqNums	" Number of times the IS has attempted to exceed the maximum sequence number." REFERENCE "{ISIS.aoi attemptsToExceedmaximumSequenceNumber (22)}"
isisSysStatAuthFails	" The number of authentication key failures recognized by this Intermediate System."
isisSysStatAuthTypeFails	" The number of authentication type mismatches recognized by this Intermediate System."
isisSysStatCorrLSPs	" Number of corrupted in-memory LSPs detected. LSPs received from the wire with a bad checksum are silently dropped and are not counted. LSPs received from the wire with parse errors are counted by isisSysStatLSPErrors." REFERENCE "{ISIS.aoi corruptedLSPsDetected (19)}"
isisSysStatIDFieldLenMismatches	" Number of times a PDU is received with a different value for ID field length from that of the receiving system." REFERENCE "{ISIS.aoi iDFieldLengthMismatches (25)}"

isisSysStatLSPDbaseOloads	" Number of times the LSP database has become overloaded." REFERENCE "{ISIS.aoi ISPL1DatabaseOverloads (20)}"
isisSysStatLSPErrors	" Number of LSPs with errors we have received."
isisSysStatManAddrDropFromAreas	" Number of times a manual address has been dropped from the area." REFERENCE "{ISIS.aoi manualAddressesDroppedFromArea (21)}"
isisSysStatOwnLSPPurges	" Number of times a zero-aged copy of the system's own LSP is received from some other node." REFERENCE "{ISIS.aoi ownLSPPurges (24)}"
isisSysStatPartChanges	" Partition changes."
isisSysStatSeqNumSkips	" Number of times a sequence number skip has occurred." REFERENCE "{ISIS.aoi sequenceNumberSkips (23)}"
isisSysStatSPFRuns	" Number of times we ran SPF at this level."
isisSysVersion	" The version number of the IS-IS protocol that is implemented." REFERENCE "{ISIS.aoi version (1)}"
isisSysWaitTime	" Number of seconds to delay in state 'waiting' before entering the state 'on'. This object follows the ResettingTimer behavior. Configured values MUST survive an agent reboot." REFERENCE "{ISIS.aoi waitingTime (15)}"

LLDP-MIB

Management Information Base module for LLDP configuration, statistics, local system data and remote systems data components.

The following table lists the tables associated with this MIB:

MIB Name	Description
lldpLocChassisId	" The string value used to identify the chassis component associated with the local system." REFERENCE " IEEE 802.1AB-2005 9.5.2.3"
lldpLocChassisIdSubtype	" The type of encoding used to identify the chassis associated with the local system." REFERENCE " IEEE 802.1AB-2005 9.5.2.2"
lldpLocManAddrIfId	" The integer value used to identify the interface number regarding the management address component associated with the local system." REFERENCE " IEEE 802.1AB-2005 9.5.9.6"
lldpLocManAddrIfSubtype	" The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system." REFERENCE " IEEE 802.1AB-2005 9.5.9.5"

lldpLocManAddrLen	" The total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP will not be required to implement an iana family numbers/address length equivalency table in order to decode the management adress." REFERENCE " IEEE 802.1AB-2005 9.5.9.2"
lldpLocPortDesc	" The string value used to identify the 802 LAN station's port description associated with the local system. If the local agent supports IETF RFC 2863, lldpLocPortDesc object should have the same value of ifDescr object." REFERENCE " IEEE 802.1AB-2005 9.5.5.2"
lldpLocPortId	" The string value used to identify the port component associated with a given port in the local system." REFERENCE " IEEE 802.1AB-2005 9.5.3.3"
lldpLocPortIdSubtype	" The type of port identifier encoding used in the associated 'lldpLocPortId' object." REFERENCE " IEEE 802.1AB-2005 9.5.3.2"
lldpLocSysCapEnabled	" The bitmap value used to identify which system capabilities are enabled on the local system." REFERENCE " IEEE 802.1AB-2005 9.5.8.2"
lldpLocSysCapSupported	" The bitmap value used to identify which system capabilities are supported on the local system." REFERENCE " IEEE 802.1AB-2005 9.5.8.1"
lldpLocSysDesc	" The string value used to identify the system description of the local system. If the local agent supports IETF RFC 3418, lldpLocSysDesc object should have the same value of sysDesc object." REFERENCE " IEEE 802.1AB-2005 9.5.7.2"
lldpLocSysName	" The string value used to identify the system name of the local system. If the local agent supports IETF RFC 3418, lldpLocSysName object should have the same value of sysName object." REFERENCE " IEEE 802.1AB-2005 9.5.6.2"
lldpRemChassisId	" The string value used to identify the chassis component associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.2.3"
lldpRemChassisIdSubtype	" The type of encoding used to identify the chassis associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.2.2"
lldpRemManAddrIfId	" The integer value used to identify the interface number regarding the management address component associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.9.6"
lldpRemManAddrIfSubtype	" The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.9.5"

lldpRemManAddrOID	" The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent." REFERENCE " IEEE 802.1AB-2005 9.5.9.8"
lldpRemPortDesc	" The string value used to identify the description of the given port associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.5.2"
lldpRemPortId	" The string value used to identify the port component associated with the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.3.3"
lldpRemPortIdSubtype	" The type of port identifier encoding used in the associated 'lldpRemPortId' object." REFERENCE " IEEE 802.1AB-2005 9.5.3.2"
lldpRemSysCapEnabled	" The bitmap value used to identify which system capabilities are enabled on the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.8.2"
lldpRemSysCapSupported	" The bitmap value used to identify which system capabilities are supported on the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.8.1"
lldpRemSysDesc	" The string value used to identify the system description of the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.7.2"
lldpRemSysName	" The string value used to identify the system name of the remote system." REFERENCE " IEEE 802.1AB-2005 9.5.6.2"

MEF-SOAM-PM-MIB

This MIB module contains the management objects for the management of Ethernet Services Operations, Administration and Maintenance for Performance Monitoring.

The following table lists the tables associated with this MIB:

MIB Name	Description

mefSoamPmMepOperNextIndex	" This object contains an unused value for a PM session number on a MEP that can be used for either LM or DM sessions, or a zero to indicate that none exist. This value needs to be read in order to find an available index for row-creation of a PM session on a MEP and then used when a row is created. This value is automatically updated by the SNMP Agent after the row is created. Referential integrity is necessary, i.e., the index needs to be persistent upon a reboot or restart of a device. The index is never to be reused for other PM sessions on the same MEP while this session is active, or until it wraps to zero. The index value keeps increasing up to that time. This is to facilitate access control based on a fixed index for an EMS, since the index is not reused. This object is an extension of the dot1agCfmMepTable and the object is automatically added or deleted based upon row creation and destruction of the dot1agCfmMepTable. "
mefSoamPmMepSlmSingleEndedResponder	" This object specifies whether the Synthetic Loss Measurement (SLM) single-ended Responder is enabled. The value 'true' indicates the single-ended SLM Responder is enabled and if a SLM message is received a SLR will be sent in reply. The value 'false' indicates the single-ended SLM Responder is disabled. If a SLM message is received no response will be sent and the message will be discarded. This object needs to be persistent upon reboot or restart of a device. A MEP can be both a single-ended Responder and Controller simultaneously. "

MPLS-LDP-STD-MIB

This MIB contains managed object definitions for the 'Multiprotocol Label Switching, Label Distribution Protocol, LDP' document."

The following table lists the tables associated with this MIB:

MIB Name	Description

mplsLdpEntityAdminStatus	" The administrative status of this LDP Entity. If this object is changed from 'enable' to 'disable' and this entity has already attempted to establish contact with a Peer, then all contact with that Peer is lost and all information from that Peer needs to be removed from the MIB. (This implies that the network management subsystem should clean up any related entry in the mplsLdpPeerTable. This further implies that a 'tear-down' for that session is issued and the session and all information related to that session cease to exist). At this point the operator is able to change values which are related to this entity. When the admin status is set back to 'enable', then this Entity will attempt to establish a new session with the Peer."
mplsLdpEntityDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this entity's counters suffered a discontinuity. The relevant counters are the specific instances associated with this entity of any Counter32 object contained in the 'mplsLdpEntityStatsTable'. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
mplsLdpEntityHelloHoldTimer	" The 16-bit integer value which is the proposed Hello hold timer for this LDP Entity. The Hello Hold time in seconds. An LSR maintains a record of Hellos received from potential peers. This object represents the Hold Time in the Common Hello Parameters TLV of the Hello Message. A value of 0 is a default value and should be interpretted in conjunction with the mplsLdpEntityTargetPeer object. If the value of this object is 0: if the value of the mplsLdpEntityTargetPeer object is false(2), then this specifies that the Hold Time's actual default value is 15 seconds (i.e., the default Hold time for Link Hellos is 15 seconds). Otherwise if the value of the mplsLdpEntityTargetPeer object is true(1), then this specifies that the Hold Time's actual default value is 45 seconds (i.e., the default Hold time for Targeted Hellos is 45 seconds). A value of 65535 means infinite (i.e., wait forever). All other values represent the amount of time in seconds to wait for a Hello Message. Setting the hold time to a value smaller than 15 is not recommended, although not forbidden according to RFC3036." REFERENCE " RFC3036, LDP Specification, Section 3.5.2., Hello Message."

mplsLdpEntityHopCountLimit	" If the value of this object is 0 (zero), then Loop Detection using Hop Counters is disabled. If the value of this object is greater than 0 (zero) then Loop Detection using Hop Counters is enabled, and this object specifies this Entity's maximum allowable value for the Hop Count. Also, the value of the object mplsLdpLsrLoopDetectionCapable must be set to either 'hopCount(3)' or 'hopCountAndPathVector(5)' if this object has a value greater than 0 (zero), otherwise it is ignored."
mplsLdpEntityIndexNext	" This object contains an appropriate value to be used for mplsLdpEntityIndex when creating entries in the mplsLdpEntityTable. The value 0 indicates that no unassigned entries are available."
mplsLdpEntityInitSessionThreshold	" When attempting to establish a session with a given Peer, the given LDP Entity should send out the SNMP notification, 'mplsLdpInitSessionThresholdExceeded', when the number of Session Initialization messages sent exceeds this threshold. The notification is used to notify an operator when this Entity and its Peer are possibly engaged in an endless sequence of messages as each NAKs the other's Initialization messages with Error Notification messages. Setting this threshold which triggers the notification is one way to notify the operator. The notification should be generated each time this threshold is exceeded and for every subsequent Initialization message which is NAK'd with an Error Notification message after this threshold is exceeded. A value of 0 (zero) for this object indicates that the threshold is infinity, thus the SNMP notification will never be generated." REFERENCE " RFC3036, LDP Specification, Section 2.5.3 Session Initialization."
mplsLdpEntityKeepAliveHoldTimer	" The 16-bit integer value which is the proposed keep alive hold timer for this LDP Entity."
mplsLdpEntityLabelDistMethod	" For any given LDP session, the method of label distribution must be specified."
mplsLdpEntityLabelRetentionMode	" The LDP Entity can be configured to use either conservative or liberal label retention mode. If the value of this object is conservative(1) then advertized label mappings are retained only if they will be used to forward packets, i.e., if label came from a valid next hop. If the value of this object is liberal(2) then all advertized label mappings are retained whether they are from a valid next hop or not."

mplsLdpEntityLabelType	" Specifies the optional parameters for the LDP Initialization Message. If the value is generic(1) then no optional parameters will be sent in the LDP Initialization message associated with this Entity. If the value is atmParameters(2) then a row must be created in the mplsLdpEntityAtmTable, which corresponds to this entry. If the value is frameRelayParameters(3) then a row must be created in the mplsLdpEntityFrameRelayTable, which corresponds to this entry." REFERENCE " RFC3036, LDP Specification, Section 3.5.3., Initialization Message."
mplsLdpEntityLastChange	" The value of sysUpTime at the time of the most recent addition or deletion of an entry to/from the mplsLdpEntityTable/mplsLdpEntityStatsTable, or the most recent change in value of any objects in the mplsLdpEntityTable. If no such changes have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
mplsLdpEntityMaxPduLength	" The maximum PDU Length that is sent in the Common Session Parameters of an Initialization Message. According to the LDP Specification [RFC3036] a value of 255 or less specifies the default maximum length of 4096 octets, this is why the value of this object starts at 256. The operator should explicitly choose the default value (i.e., 4096), or some other value. The receiving LSR MUST calculate the maximum PDU length for the session by using the smaller of its and its peer's proposals for Max PDU Length." REFERENCE " RFC3036, LDP Specification, Section 3.5.3. Initialization Message."
mplsLdpEntityOperStatus	" The operational status of this LDP Entity. The value of unknown(1) indicates that the operational status cannot be determined at this time. The value of unknown should be a transient condition before changing to enabled(2) or disabled(3)."
mplsLdpEntityPathVectorLimit	" If the value of this object is 0 (zero) then Loop Detection for Path Vectors is disabled. Otherwise, if this object has a value greater than zero, then Loop Dection for Path Vectors is enabled, and the Path Vector Limit is this value. Also, the value of the object, 'mplsLdpLsrLoopDetectionCapable', must be set to either 'pathVector(4)' or 'hopCountAndPathVector(5)', if this object has a value greater than 0 (zero), otherwise it is ignored." REFERENCE " RFC3036, LDP Specification, Section 2.8 Loop Dection, Section 3.4.5 Path Vector TLV."

mplsLdpEntityProtocolVersion	" The version number of the LDP protocol which will be used in the session initialization message. Section 3.5.3 in the LDP Specification specifies that the version of the LDP protocol is negotiated during session establishment. The value of this object represents the value that is sent in the initialization message." REFERENCE " RFC3036, LDP Specification, Section 3.5.3 Initialization Message."
mplsLdpEntityRowStatus	" The status of this conceptual row. All writable objects in this row may be modified at any time, however, as described in detail in the section entitled, 'Changing Values After Session Establishment', and again described in the DESCRIPTION clause of the mplsLdpEntityAdminStatus object, if a session has been initiated with a Peer, changing objects in this table will wreak havoc with the session and interrupt traffic. To repeat again: the recommended procedure is to set the mplsLdpEntityAdminStatus to down, thereby explicitly causing a session to be torn down. Then, change objects in this entry, then set the mplsLdpEntityAdminStatus to enable, which enables a new session to be initiated."
mplsLdpEntityStatsBadLdpIdentifierErrors	" This object counts the number of Bad LDP Identifier Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."
mplsLdpEntityStatsBadMessageLengthErrors	" This object counts the number of Bad Message Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."
mplsLdpEntityStatsBadPduLengthErrors	" This object counts the number of Bad PDU Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."

mplsLdpEntityStatsBadTlvLengthErrors	" This object counts the number of Bad TLV Length Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."
mplsLdpEntityStatsKeepAliveTimerExpErrors	" This object counts the number of Session Keep Alive Timer Expired Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."
mplsLdpEntityStatsMalformedTlvValueErrors	" This object counts the number of Malformed TLV Value Fatal Errors detected by the session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime." REFERENCE " RFC3036, LDP Specification, Section 3.5.1.2."
mplsLdpEntityStatsSessionAttempts	" A count of the Session Initialization messages which were sent or received by this LDP Entity and were NAK'd. In other words, this counter counts the number of session initializations that failed. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStatsSessionRejectedAdErrors	" A count of the Session Rejected/Parameters Advertisement Mode Error Notification Messages sent or received by this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStatsSessionRejectedLRErrors	" A count of the Session Rejected/Parameters Label Range Notification Messages sent or received by this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."

mplsLdpEntityStatsSessionRejectedMaxPduErrors	" A count of the Session Rejected/Parameters Max Pdu Length Error Notification Messages sent or received by this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStatsSessionRejectedNoHelloErrors	" A count of the Session Rejected/No Hello Error Notification Messages sent or received by this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStatsShutdownReceivedNotifications	" This object counts the number of Shutdown Notifications received related to session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStatsShutdownSentNotifications	" This object counts the number of Shutdown Notfications sent related to session(s) (past and present) associated with this LDP Entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime."
mplsLdpEntityStorageType	" The storage type for this conceptual row. Conceptual rows having the value 'permanent(4)' need not allow write-access to any columnar objects in the row."
mplsLdpEntityTargetPeer	" If this LDP entity uses targeted peer then set this to true."
mplsLdpEntityTargetPeerAddr	" The value of the internetwork layer address used for the Extended Discovery. The value of mplsLdpEntityTargetPeerAddrType specifies how this address is to be interpreted."
mplsLdpEntityTargetPeerAddrType	" The type of the internetwork layer address used for the Extended Discovery. This object indicates how the value of mplsLdpEntityTargetPeerAddr is to be interpreted."
mplsLdpEntityTcpPort	" The TCP Port for LDP. The default value is the well-known value of this port." REFERENCE " RFC3036, LDP Specification, Section 3.10, Well-known Numbers, and Section 3.10.1. UDP and TCP Ports."

mplsLdpEntityTransportAddrKind	" This specifies whether the loopback or interface address is to be used as the transport address in the transport address TLV of the hello message. If the value is interface(1), then the IP address of the interface from which hello messages are sent is used as the transport address in the hello message. Otherwise, if the value is loopback(2), then the IP address of the loopback interface is used as the transport address in the hello message."
mplsLdpEntityUdpDscPort	" The UDP Discovery Port for LDP. The default value is the well-known value for this port." REFERENCE " RFC3036, LDP Specification, Section 2.4.1, Basic Discovery Mechanism, Section 2.4.2, Extended Discovery Mechanism, Section 3.10, Well-known Numbers, and Section 3.10.1. UDP and TCP Ports."
mplsLdpHelloAdjacencyHoldTime	" The Hello hold time which is negotiated between the Entity and the Peer. The entity associated with this Hello Adjacency issues a proposed Hello Hold Time value in the mplsLdpEntityHelloHoldTimer object. The peer also proposes a value and this object represents the negotiated value. A value of 0 means the default, which is 15 seconds for Link Hellos and 45 seconds for Targeted Hellos. A value of 65535 indicates an infinite hold time." REFERENCE " RFC3036, LDP Specification, Section 3.5.2 Hello Message"
mplsLdpHelloAdjacencyHoldTimeRem	" If the value of this object is 65535, this means that the hold time is infinite (i.e., wait forever). Otherwise, the time remaining for this Hello Adjacency to receive its next Hello Message. This interval will change when the 'next' Hello Message which corresponds to this Hello Adjacency is received unless it is infinite."
mplsLdpHelloAdjacencyType	" This adjacency is the result of a 'link' hello if the value of this object is link(1). Otherwise, it is a result of a 'targeted' hello, targeted(2)."
mplsLdpLspFecLastChange	" The value of sysUpTime at the time of the most recent addition/deletion of an entry to/from the mplsLdpLspFecTable or the most recent change in values to any objects in the mplsLdpLspFecTable. If no such changes have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
mplsLdpLsrId	" The Label Switching Router's Identifier."

mplsLdpLsrLoopDetectionCapable	" A indication of whether this Label Switching Router supports loop detection. none(1) -- Loop Detection is not supported on this LSR. other(2) -- Loop Detection is supported but by a method other than those listed below. hopCount(3) -- Loop Detection is supported by Hop Count only. pathVector(4) -- Loop Detection is supported by Path Vector only. hopCountAndPathVector(5) -- Loop Detection is supported by both Hop Count And Path Vector. Since Loop Detection is determined during Session Initialization, an individual session may not be running with loop detection. This object simply gives an indication of whether or not the LSR has the ability to support Loop Detection and which types."
mplsLdpPeerLabelDistMethod	" For any given LDP session, the method of label distribution must be specified."
mplsLdpPeerLastChange	" The value of sysUpTime at the time of the most recent addition or deletion to/from the mplsLdpPeerTable/mplsLdpSessionTable."
mplsLdpPeerPathVectorLimit	" If the value of this object is 0 (zero) then Loop Dection for Path Vectors for this Peer is disabled. Otherwise, if this object has a value greater than zero, then Loop Dection for Path Vectors for this Peer is enabled and the Path Vector Limit is this value." REFERENCE " RFC3036, LDP Specification, Section 2.8 Loop Dection, Section 3.4.5 Path Vector TLV."
mplsLdpPeerTransportAddr	" The Internet address advertised by the peer in the Hello Message or the Hello source address. The type of this address is specified by the value of the mplsLdpPeerTransportAddrType object." REFERENCE " RFC3036, LDP Specification, Section 2.5.2 Transport Connection Establishment and Section 3.5.2.1 Hello Message Procedures."
mplsLdpPeerTransportAddrType	" The type of the Internet address for the mplsLdpPeerTransportAddr object. The LDP specification describes this as being either an IPv4 Transport Address or IPv6 Transport Address which is used in opening the LDP session's TCP connection, or if the optional TLV is not present, then this is the IPv4/IPv6 source address for the UPD packet carrying the Hellos. This object specifies how the value of the mplsLdpPeerTransportAddr object should be interpreted." REFERENCE " RFC3036, LDP Specification, Section 2.5.2 Transport Connection Establishment and Section 3.5.2.1 Hello Message Procedures."

mplsLdpSessionDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this session's counters suffered a discontinuity. The relevant counters are the specific instances associated with this session of any Counter32 object contained in the mplsLdpSessionStatsTable. The initial value of this object is the value of sysUpTime when the entry was created in this table. Also, a command generator can distinguish when a session between a given Entity and Peer goes away and a new session is established. This value would change and thus indicate to the command generator that this is a different session."
mplsLdpSessionKeepAliveHoldTimeRem	" The keep alive hold time remaining for this session."
mplsLdpSessionKeepAliveTime	" The negotiated KeepAlive Time which represents the amount of seconds between keep alive messages. The mplsLdpEntityKeepAliveHoldTimer related to this Session is the value that was proposed as the KeepAlive Time for this session. This value is negotiated during session initialization between the entity's proposed value (i.e., the value configured in mplsLdpEntityKeepAliveHoldTimer) and the peer's proposed KeepAlive Hold Timer value. This value is the smaller of the two proposed values." REFERENCE " RFC3036, LDP Specification, Section 3.5.3, Initialization Message."
mplsLdpSessionMaxPduLength	" The value of maximum allowable length for LDP PDUs for this session. This value may have been negotiated during the Session Initialization. This object is related to the mplsLdpEntityMaxPduLength object. The mplsLdpEntityMaxPduLength object specifies the requested LDP PDU length, and this object reflects the negotiated LDP PDU length between the Entity and the Peer." REFERENCE " RFC3036, LDP Specification, Section 3.5.3, Initialization Message."
mplsLdpSessionPeerNextHopAddr	" The next hop address. The type of this address is specified by the value of the mplsLdpSessionPeerNextHopAddrType." REFERENCE " RFC3036, Section 2.7. LDP Identifiers and Next Hop Addresses"
mplsLdpSessionPeerNextHopAddrType	" The internetwork layer address type of this Next Hop Address as specified in the Label Address Message associated with this Session. The value of this object indicates how to interpret the value of mplsLdpSessionPeerNextHopAddr."

mplsLdpSessionProtocolVersion	" The version of the LDP Protocol which this session is using. This is the version of the LDP protocol which has been negotiated during session initialization." REFERENCE " RFC3036, LDP Specification, Section 3.5.3, Initialization Message."
mplsLdpSessionRole	" During session establishment the LSR/LER takes either the active role or the passive role based on address comparisons. This object indicates whether this LSR/LER was behaving in an active role or passive role during this session's establishment. The value of unknown(1), indicates that the role is not able to be determined at the present time." REFERENCE " RFC3036, LDP Specification, Section 2.5.3., Session Initialization"
mplsLdpSessionState	" The current state of the session, all of the states 1 to 5 are based on the state machine for session negotiation behavior." REFERENCE " RFC3036, LDP Specification, Section 2.5.4, Initialization State Machine."
mplsLdpSessionStateLastChange	" The value of sysUpTime at the time this Session entered its current state as denoted by the mplsLdpSessionState object."
mplsLdpSessionStatsUnknownMesTypeErrors	" This object counts the number of Unknown Message Type Errors detected by this LSR/LER during this session. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpSessionDiscontinuityTime."
mplsLdpSessionStatsUnknownTlvErrors	" This object counts the number of Unknown TLV Errors detected by this LSR/LER during this session. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpSessionDiscontinuityTime."
mplsFecIndexNext	" This object contains an appropriate value to be used for mplsFecIndex when creating entries in the mplsFecTable. The value 0 indicates that no unassigned entries are available."
mplsFecLastChange	" The value of sysUpTime at the time of the most recent addition/deletion of an entry to/from the mplsLdpFectTable or the most recent change in values to any objects in the mplsLdpFecTable. If no such changes have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."

MPLS-LSR-STD-MIB

This MIB module contains managed object definitions for the Multiprotocol Label Switching (MPLS) Router as defined in: Rosen, E., Viswanathan, A., and R Callon, Multiprotocol Label Switching Architecture, RFC 3031, January 2001.

The following table lists the tables associated with this MIB:

MIB Name	Description
mplsInSegmentAddrFamily	" The IANA address family [IANAFamily] of packets received on this segment, which is used at an egress LSR to deliver them to the appropriate layer 3 entity. A value of other(0) indicates that the family type is either unknown or undefined; this SHOULD NOT be used at an egress LSR. This object cannot be modified if mplsInSegmentRowStatus is active(1)." REFERENCE " Internet Assigned Numbers Authority (IANA), ADDRESS FAMILY NUMBERS, (http://www.iana.org/assignments/ address-family-numbers), for MIB see: http://www.iana.org/assignments/ ianaaddressfamilynumbers-mib "
mplsInSegmentIndexNext	" This object contains the next available value to be used for mplsInSegmentIndex when creating entries in the mplsInSegmentTable. The special value of a string containing the single octet 0x00 indicates that no new entries can be created in this table. Agents not allowing managers to create entries in this table MUST set this object to this special value."
mplsInSegmentInterface	" This object represents the interface index for the incoming MPLS interface. A value of zero represents all interfaces participating in the per-platform label space. This may only be used in cases where the incoming interface and label are associated with the same mplsXCEntry. Specifically, given a label and any incoming interface pair from the per-platform label space, the outgoing label/interface mapping remains the same. If this is not the case, then individual entries MUST exist that can then be mapped to unique mplsXCEntries."
mplsInSegmentLabel	" If the corresponding instance of mplsInSegmentLabelPtr is zeroDotZero then this object MUST contain the incoming label associated with this in-segment. If not this object SHOULD be zero and MUST be ignored."

mplsInSegmentLabelPtr	" If the label for this segment cannot be represented fully within the mplsInSegmentLabel object, this object MUST point to the first accessible column of a conceptual row in an external table containing the label. In this case, the mplsInSegmentTopLabel object SHOULD be set to 0 and ignored. This object MUST be set to zeroDotZero otherwise."
mplsInSegmentNPop	" The number of labels to pop from the incoming packet. Normally only the top label is popped from the packet and used for all switching decisions for that packet. This is indicated by setting this object to the default value of 1. If an LSR supports popping of more than one label, this object MUST be set to that number. This object cannot be modified if mplsInSegmentRowStatus is active(1)."
mplsInSegmentOwner	" Denotes the entity that created and is responsible for managing this segment."
mplsInSegmentPerfDiscards	" The number of labeled packets received on this in-segment, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a labeled packet could be to free up buffer space."
mplsInSegmentPerfDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this segment's Counter32 or Counter64 suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
mplsInSegmentPerfErrors	" The number of errored packets received on this segment."
mplsInSegmentPerfHCOctets	" The total number of octets received. This is the 64 bit version of mplsInSegmentPerfOctets, if mplsInSegmentPerfHCOctets is supported according to the rules spelled out in RFC2863."
mplsInSegmentPerfOctets	" This value represents the total number of octets received by this segment. It MUST be equal to the least significant 32 bits of mplsInSegmentPerfHCOctets if mplsInSegmentPerfHCOctets is supported according to the rules spelled out in RFC2863."
mplsInSegmentPerfPackets	" Total number of packets received by this segment."
mplsInSegmentRowStatus	" This variable is used to create, modify, and/or delete a row in this table. When a row in this table has a row in the active(1) state, no objects in this row can be modified except the mplsInSegmentRowStatus and mplsInSegmentStorageType."
mplsInSegmentStorageType	" This variable indicates the storage type for this object. The agent MUST ensure that this object's value remains consistent with the associated mplsXCEntry. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row." REFERENCE " See RFC2579."

mplsInSegmentTrafficParamPtr	" This variable represents a pointer to the traffic parameter specification for this in-segment. This value may point at an entry in the mplsTunnelResourceTable in the MPLS-TE-STD-MIB (RFC3812) to indicate which traffic parameter settings for this segment if it represents an LSP used for a TE tunnel. This value may optionally point at an externally defined traffic parameter specification table. A value of zeroDotZero indicates best-effort treatment. By having the same value of this object, two or more segments can indicate resource sharing of such things as LSP queue space, etc. This object cannot be modified if mplsInSegmentRowStatus is active(1). For entries in this table that are preserved after a re-boot, the agent MUST ensure that their integrity be preserved, or this object should be set to 0.0 if it cannot."
mplsInSegmentXCIndex	" Index into mplsXCTable which identifies which cross-connect entry this segment is part of. The string containing the single octet 0x00 indicates that this entry is not referred to by any cross-connect entry. When a cross-connect entry is created which this in-segment is a part of, this object is automatically updated to reflect the value of mplsXCIndex of that cross-connect entry."
mplsInterfaceAvailableBandwidth	" This value indicates the total amount of available bandwidth available on this interface and is specified in kilobits per second (Kbps). This value is calculated as the difference between the amount of bandwidth currently in use and that specified in mplsInterfaceTotalBandwidth. This variable is not applicable when applied to the interface with index 0. When this value cannot be measured, this value should contain the nominal bandwidth."
mplsInterfaceLabelMaxIn	" This is the maximum value of an MPLS label that this LSR is willing to receive on this interface."
mplsInterfaceLabelMaxOut	" This is the maximum value of an MPLS label that this LSR is willing to send on this interface."
mplsInterfaceLabelMinIn	" This is the minimum value of an MPLS label that this LSR is willing to receive on this interface."
mplsInterfaceLabelMinOut	" This is the minimum value of an MPLS label that this LSR is willing to send on this interface."

mplsInterfaceLabelParticipationType	" If the value of the mplsInterfaceIndex for this entry is zero, then this entry corresponds to the per-platform label space for all interfaces configured to use that label space. In this case the perPlatform(0) bit MUST be set; the perInterface(1) bit is meaningless and MUST be ignored. The remainder of this description applies to entries with a non-zero value of mplsInterfaceIndex. If the perInterface(1) bit is set then the value of mplsInterfaceLabelMinIn, mplsInterfaceLabelMaxIn, mplsInterfaceLabelMinOut, and mplsInterfaceLabelMaxOut for this entry reflect the label ranges for this interface. If only the perPlatform(0) bit is set, then the value of mplsInterfaceLabelMinIn, mplsInterfaceLabelMaxIn, mplsInterfaceLabelMinOut, and mplsInterfaceLabelMaxOut for this entry MUST be identical to the instance of these objects with index 0. These objects may only vary from the entry with index 0 if both the perPlatform(0) and perInterface(1) bits are set. In all cases, at a minimum one of the perPlatform(0) or perInterface(1) bits MUST be set to indicate that at least one label space is in use by this interface. In all cases, agents MUST ensure that label ranges are specified consistently and MUST return an inconsistentValue error when they do not." REFERENCE " Rosen, E., Viswanathan, A., and R. Callon, Multiprotocol Label Switching Architecture, RFC 3031, January 2001."
mplsInterfacePerfInLabelLookupFailures	" This object counts the number of labeled packets that have been received on this interface and which were discarded because there was no matching cross- connect entry. This object MUST count on a per- interface basis regardless of which label space the interface participates in."
mplsInterfacePerfInLabelsInUse	" This object counts the number of labels that are in use at this point in time on this interface in the incoming direction. If the interface participates in only the per-platform label space, then the value of the instance of this object MUST be identical to the value of the instance with index 0. If the interface participates in the per-interface label space, then the instance of this object MUST represent the number of per-interface labels that are in use on this interface."
mplsInterfacePerfOutFragmentedPkts	" This object counts the number of outgoing MPLS packets that required fragmentation before transmission on this interface. This object MUST count on a per-interface basis regardless of which label space the interface participates in."
mplsInterfacePerfOutLabelsInUse	" This object counts the number of top-most labels in the outgoing label stacks that are in use at this point in time on this interface. This object MUST count on a per-interface basis regardless of which label space the interface participates in."

mplsInterfaceTotalBandwidth	" This value indicates the total amount of usable bandwidth on this interface and is specified in kilobits per second (Kbps). This variable is not applicable when applied to the interface with index 0. When this value cannot be measured, this value should contain the nominal bandwidth."
mplsLabelStackIndexNext	" This object contains the next available value to be used for mplsLabelStackIndex when creating entries in the mplsLabelStackTable. The special string containing the single octet 0x00 indicates that no more new entries can be created in the relevant table. Agents not allowing managers to create entries in this table MUST set this value to the string containing the single octet 0x00."
mplsMaxLabelStackDepth	" The maximum stack depth supported by this LSR."
mplsOutSegmentIndexNext	" This object contains the next available value to be used for mplsOutSegmentIndex when creating entries in the mplsOutSegmentTable. The special value of a string containing the single octet 0x00 indicates that no new entries can be created in this table. Agents not allowing managers to create entries in this table MUST set this object to this special value."
mplsOutSegmentInterface	" This value must contain the interface index of the outgoing interface. This object cannot be modified if mplsOutSegmentRowStatus is active(1). The mplsOutSegmentRowStatus cannot be set to active(1) until this object is set to a value corresponding to a valid ifEntry."
mplsOutSegmentNextHopAddr	" The internet address of the next hop. The type of this address is determined by the value of the mplslOutSegmentNextHopAddrType object. This object cannot be modified if mplsOutSegmentRowStatus is active(1)."
mplsOutSegmentNextHopAddrType	" Indicates the next hop Internet address type. Only values unknown(0), ipv4(1) or ipv6(2) have to be supported. A value of unknown(0) is allowed only when the outgoing interface is of type point-to-point. If any other unsupported values are attempted in a set operation, the agent MUST return an inconsistentValue error." REFERENCE " See RFC3291."
mplsOutSegmentOwner	" Denotes the entity which created and is responsible for managing this segment."
mplsOutSegmentPerfDiscards	" The number of labeled packets attempted to be transmitted on this out-segment, which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a labeled packet could be to free up buffer space."

mplsOutSegmentPerfDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one or more of this segment's Counter32 or Counter64 suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
mplsOutSegmentPerfErrors	" Number of packets that could not be sent due to errors on this segment."
mplsOutSegmentPerfHCOctets	" Total number of octets sent. This is the 64 bit version of mplsOutSegmentPerfOctets, if mplsOutSegmentPerfHCOctets is supported according to the rules spelled out in RFC2863."
mplsOutSegmentPerfOctets	" This value contains the total number of octets sent on this segment. It MUST be equal to the least significant 32 bits of mplsOutSegmentPerfHCOctets if mplsOutSegmentPerfHCOctets is supported according to the rules spelled out in RFC2863."
mplsOutSegmentPerfPackets	" This value contains the total number of packets sent on this segment."
mplsOutSegmentPushTopLabel	" This value indicates whether or not a top label should be pushed onto the outgoing packet's label stack. The value of this variable MUST be set to true(1) if the outgoing interface does not support pop-and-go (and no label stack remains). For example, on ATM interface, or if the segment represents a tunnel origination. Note that it is considered an error in the case that mplsOutSegmentPushTopLabel is set to false, but the cross-connect entry which refers to this out-segment has a non-zero mplsLabelStackIndex. The LSR MUST ensure that this situation does not happen. This object cannot be modified if mplsOutSegmentRowStatus is active(1)."
mplsOutSegmentRowStatus	" For creating, modifying, and deleting this row. When a row in this table has a row in the active(1) state, no objects in this row can be modified except the mplsOutSegmentRowStatus or mplsOutSegmentStorageType."
mplsOutSegmentStorageType	" This variable indicates the storage type for this object. The agent MUST ensure that this object's value remains consistent with the associated mplsXCEntry. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row."
mplsOutSegmentTopLabel	" If mplsOutSegmentPushTopLabel is true then this represents the label that should be pushed onto the top of the outgoing packet's label stack. Otherwise this value SHOULD be set to 0 by the management station and MUST be ignored by the agent. This object cannot be modified if mplsOutSegmentRowStatus is active(1)."

mplsOutSegmentTopLabelPtr	" If the label for this segment cannot be represented fully within the mplsOutSegmentLabel object, this object MUST point to the first accessible column of a conceptual row in an external table containing the label. In this case, the mplsOutSegmentTopLabel object SHOULD be set to 0 and ignored. This object MUST be set to zeroDotZero otherwise."
mplsOutSegmentTrafficParamPtr	" This variable represents a pointer to the traffic parameter specification for this out-segment. This value may point at an entry in the MplsTunnelResourceEntry in the MPLS-TE-STD-MIB (RFC3812) RFC Editor: Please fill in RFC number. to indicate which traffic parameter settings for this segment if it represents an LSP used for a TE tunnel. This value may optionally point at an externally defined traffic parameter specification table. A value of zeroDotZero indicates best-effort treatment. By having the same value of this object, two or more segments can indicate resource sharing of such things as LSP queue space, etc. This object cannot be modified if mplsOutSegmentRowStatus is active(1). For entries in this table that are preserved after a re-boot, the agent MUST ensure that their integrity be preserved, or this object should be set to 0.0 if it cannot."
mplsOutSegmentXCIndex	" Index into mplsXCTable which identifies which cross-connect entry this segment is part of. A value of the string containing the single octet 0x00 indicates that this entry is not referred to by any cross-connect entry. When a cross-connect entry is created which this out-segment is a part of, this object MUST be updated by the agent to reflect the value of mplsXCIndex of that cross-connect entry."

MPLS-LDP-GENERIC-STD-MIB

This MIB contains managed object definitions for configuring and monitoring the Multiprotocol Label

Switching (MPLS), Label Distribution Protocol (LDP) utilizing ethernet as the Layer 2 media."

The following table lists the tables associated with this MIB:

MIB Name	Description

mplsLdpEntityGenericIfIndexOrZero	" This value represents either the InterfaceIndex of the 'ifLayer' where these Generic Label would be created, or 0 (zero). The value of zero means that the InterfaceIndex is not known. However, if the InterfaceIndex is known, then it must be represented by this value. If an InterfaceIndex becomes known, then the network management entity (e.g., SNMP agent) responsible for this object MUST change the value from 0 (zero) to the value of the InterfaceIndex."
mplsLdpEntityGenericLabelSpace	" This value of this object is perPlatform(1), then this means that the label space type is per platform. If this object is perInterface(2), then this means that the label space type is per Interface." REFERENCE " RFC3036, LDP Specification, Section 2.2.1, Label Spaces."
mplsLdpEntityGenericLRRowStatus	" The status of this conceptual row. All writable objects in this row may be modified at any time, however, as described in detail in the section entitled, 'Changing Values After Session Establishment', and again described in the DESCRIPTION clause of the mplsLdpEntityAdminStatus object, if a session has been initiated with a Peer, changing objects in this table will wreak havoc with the session and interrupt traffic. To repeat again: the recommended procedure is to set the mplsLdpEntityAdminStatus to down, thereby explicitly causing a session to be torn down. Then, change objects in this entry, then set the mplsLdpEntityAdminStatus to enable which enables a new session to be initiated. There must exist at least one entry in this table for every LDP Entity that has a generic label configured."
mplsLdpEntityGenericLRStorageType	" The storage type for this conceptual row. Conceptual rows having the value 'permanent(4)' need not allow write-access to any columnar objects in the row."

MPLS-TE-STD-MIB

This MIB module contains managed object definition for MPLS Traffic Engineering (TE).

The following table lists the tables associated with this MIB:

MIB Name	Description
mplsTunnelActive	" The number of tunnels active on this device. A tunnel is considered active if the mplsTunnelOperStatus is up(1)."
mplsTunnelAdminStatus	" Indicates the desired operational status of this tunnel."

mplsTunnelARHopAddrType	" The Hop Address Type of this tunnel hop. Note that lspid(5) is a valid option only for tunnels signaled via CRLDP."
mplsTunnelARHopAddrUnnum	" If mplsTunnelARHopAddrType is set to unnum(4), then this value will contain the interface identifier of the unnumbered interface for this hop. This object should be used in conjunction with mplsTunnelARHopIpAddr which would contain the LSR Router ID in this case. Otherwise the agent should set this object to zero-length string and the manager should ignore this."
mplsTunnelARHopIpAddr	" The Tunnel Hop Address for this tunnel hop. The type of this address is determined by the value of the corresponding mplsTunnelARHopAddrType. If mplsTunnelARHopAddrType is set to unnum(4), then this value contains the LSR Router ID of the unnumbered interface. Otherwise the agent SHOULD set this object to the zero-length string and the manager should ignore this object."
mplsTunnelARHopLspId	" If mplsTunnelARHopAddrType is set to lspid(5), then this value will contain the LSP ID of this hop. This object is otherwise insignificant and should contain a value of 0 to indicate this fact."
mplsTunnelARHopTableIndex	" Index into the mplsTunnelARHopTable entry that specifies the actual hops traversed by the tunnel. This is automatically updated by the agent when the actual hops becomes available."
mplsTunnelCHopAddrType	" The Hop Address Type of this tunnel hop. Note that lspid(5) is a valid option only for tunnels signaled via CRLDP."
mplsTunnelCHopAddrUnnum	" If mplsTunnelCHopAddrType is set to unnum(4), then this value will contain the unnumbered interface identifier of this hop. This object should be used in conjunction with mplsTunnelCHopIpAddr which would contain the LSR Router ID in this case. Otherwise the agent should set this object to zero-length string and the manager should ignore this."
mplsTunnelCHopAsNumber	" If mplsTunnelCHopAddrType is set to asnumber(3), then this value will contain the AS number of this hop. Otherwise the agent should set this object to zero-length string and the manager should ignore this."
mplsTunnelCHopIpAddr	" The Tunnel Hop Address for this tunnel hop. The type of this address is determined by the value of the corresponding mplsTunnelCHopAddrType. If mplsTunnelCHopAddrType is set to unnum(4), then this value will contain the LSR Router ID of the unnumbered interface. Otherwise the agent should set this object to the zero-length string and the manager SHOULD ignore this object."
mplsTunnelCHopIpPrefixLen	" If mplsTunnelCHopAddrType is set to ipv4(1) or ipv6(2), then this value will contain an appropriate prefix length for the IP address in object mplsTunnelCHopIpAddr. Otherwise this value is irrelevant and should be ignored. "

mplsTunnelCHopLspId	" If mplsTunnelCHopAddrType is set to lspid(5), then this value will contain the LSP ID of this hop. This object is otherwise insignificant and should contain a value of 0 to indicate this fact."
mplsTunnelCHopTableIndex	" Index into the mplsTunnelCHopTable entry that specifies the computed hops traversed by the tunnel. This is automatically updated by the agent when computed hops become available or when computed hops get modified."
mplsTunnelCHopType	" Denotes whether this is tunnel hop is routed in a strict or loose fashion."
mplsTunnelConfigured	" The number of tunnels configured on this device. A tunnel is considered configured if the mplsTunnelRowStatus is active(1)."
mplsTunnelCreationTime	" Specifies the value of SysUpTime when the first instance of this tunnel came into existence. That is, when the value of mplsTunnelOperStatus was first set to up(1)."
mplsTunnelDescr	" A textual string containing information about the tunnel. If there is no description this object contains a zero length string. This object is may not be signaled by MPLS signaling protocols, consequentally the value of this object at transit and egress LSRs MAY be automatically generated or absent."
mplsTunnelExcludeAnyAffinity	" A link satisfies the exclude-any constraint if and only if the link contains none of the administrative groups specified in the constraint." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
mplsTunnelHoldingPrio	" Indicates the holding priority for this tunnel." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001 2. Constraint-Based LSP Setup using LDP, Jamoussi (Editor), RFC 3212, January 2002"
mplsTunnelHopAddrType	" The Hop Address Type of this tunnel hop. The value of this object cannot be changed if the value of the corresponding mplsTunnelHopRowStatus object is 'active'. Note that lspid(5) is a valid option only for tunnels signaled via CRLDP. "
mplsTunnelHopAddrUnnum	" If mplsTunnelHopAddrType is set to unnum(4), then this value will contain the interface identifier of the unnumbered interface for this hop. This object should be used in conjunction with mplsTunnelHopIpAddress which would contain the LSR Router ID in this case. Otherwise the agent should set this object to zero-length string and the manager should ignore this."
mplsTunnelHopAsNumber	" If mplsTunnelHopAddrType is set to asnumber(3), then this value will contain the AS number of this hop. Otherwise the agent should set this object to zero-length string and the manager should ignore this."

mplsTunnelHopEntryPathComp	" If this value is set to dynamic, then the user should only specify the source and destination of the path and expect that the CSPF will calculate the remainder of the path. If this value is set to explicit, the user should specify the entire path for the tunnel to take. This path may contain strict or loose hops. Each hop along a specific path SHOULD have this object set to the same value"
mplsTunnelHopInclude	" If this value is set to true, then this indicates that this hop must be included in the tunnel's path. If this value is set to 'false', then this hop must be avoided when calculating the path for this tunnel. The default value of this object is 'true', so that by default all indicated hops are included in the CSPF path computation. If this object is set to 'false' the value of mplsTunnelHopType should be ignored."
mplsTunnelHopIpAddr	" The Tunnel Hop Address for this tunnel hop. The type of this address is determined by the value of the corresponding mplsTunnelHopAddrType. The value of this object cannot be changed if the value of the corresponding mplsTunnelHopRowStatus object is 'active'. "
mplsTunnelHopIpPrefixLen	" If mplsTunnelHopAddrType is set to ipv4(1) or ipv6(2), then this value will contain an appropriate prefix length for the IP address in object mplsTunnelHopIpAddr. Otherwise this value is irrelevant and should be ignored. "
mplsTunnelHopListIndexNext	" This object contains an appropriate value to be used for mplsTunnelHopListIndex when creating entries in the mplsTunnelHopTable. If the number of unassigned entries is exhausted, a retrieval operation will return a value of 0. This object may also return a value of 0 when the LSR is unable to accept conceptual row creation, for example, if the mplsTunnelHopTable is implemented as read-only. To obtain the value of mplsTunnelHopListIndex for a new entry in the mplsTunnelHopTable, the manager issues a management protocol retrieval operation to obtain the current value of mplsTunnelHopIndex. When the SET is performed to create a row in the mplsTunnelHopTable, the Command Responder (agent) must determine whether the value is indeed still unused; Two Network Management Applications may attempt to create a row (configuration entry) simultaneously and use the same value. If it is currently unused, the SET succeeds and the Command Responder (agent) changes the value of this object, according to an implementation-specific algorithm. If the value is in use, however, the SET fails. The Network Management Application must then re-read this variable to obtain a new usable value."

mplsTunnelHopLspId	" If mplsTunnelHopAddrType is set to lspid(5), then this value will contain the LSPID of a tunnel of this hop. The present tunnel being configured is tunneled through this hop (using label stacking). This object is otherwise insignificant and should contain a value of 0 to indicate this fact."
mplsTunnelHopPathOptionName	" The description of this series of hops as they relate to the specified path option. The value of this object SHOULD be the same for each hop in the series that comprises a path option."
mplsTunnelHopRowStatus	" This variable is used to create, modify, and/or delete a row in this table. When a row in this table is in active(1) state, no objects in that row can be modified by the agent except mplsTunnelHopRowStatus and mplsTunnelHopStorageType."
mplsTunnelHopStorageType	" The storage type for this Hop entry. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row."
mplsTunnelHopTableIndex	" Index into the mplsTunnelHopTable entry that specifies the explicit route hops for this tunnel. This object is meaningful only at the head-end of the tunnel."
mplsTunnelHopType	" Denotes whether this tunnel hop is routed in a strict or loose fashion. The value of this object has no meaning if the mplsTunnelHopInclude object is set to 'false'."
mplsTunnelIfIndex	" If mplsTunnelIsIf is set to true, then this value contains the LSR-assigned ifIndex which corresponds to an entry in the interfaces table. Otherwise this variable should contain the value of zero indicating that a valid ifIndex was not assigned to this tunnel interface." REFERENCE " RFC 2863 - The Interfaces Group MIB, McCloghrie, K., and F. Kastenholtz, June 2000"
mplsTunnelIncludeAllAffinity	" A link satisfies the include-all constraint if and only if the link contains all of the administrative groups specified in the constraint." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
mplsTunnelIncludeAnyAffinity	" A link satisfies the include-any constraint if and only if the constraint is zero, or the link and the constraint have a resource class in common." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
mplsTunnelIndexNext	" This object contains an unused value for mplsTunnelIndex, or a zero to indicate that none exist. Negative values are not allowed, as they do not correspond to valid values of mplsTunnelIndex. Note that this object offers an unused value for an mplsTunnelIndex value at the ingress side of a tunnel. At other LSRs the value of mplsTunnelIndex SHOULD be taken from the value signaled by the MPLS signaling protocol. "

mplsTunnelInstancePriority	" This value indicates which priority, in descending order, with 0 indicating the lowest priority, within a group of tunnel instances. A group of tunnel instances is defined as a set of LSPs with the same mplsTunnelIndex in this table, but with a different mplsTunnelInstance. Tunnel instance priorities are used to denote the priority at which a particular tunnel instance will supercede another. Instances of tunnels containing the same mplsTunnelInstancePriority will be used for load sharing."
mplsTunnelInstanceUpTime	" This value identifies the total time that this tunnel instance's operStatus has been Up(1)."
mplsTunnelIsIf	" Denotes whether or not this tunnel corresponds to an interface represented in the interfaces group table. Note that if this variable is set to true then the ifName of the interface corresponding to this tunnel should have a value equal to mplsTunnelName. Also see the description of ifName in RFC 2863. This object is meaningful only at the ingress and egress LSRs." REFERENCE " RFC 2863 - The Interfaces Group MIB, McCloghrie, K., and F. Kastenholtz, June 2000"
mplsTunnelLastPathChange	" Specifies the time since the last change to the actual path for this tunnel instance."
mplsTunnelLocalProtectInUse	" Indicates that the local repair mechanism is in use to maintain this tunnel (usually in the face of an outage of the link it was previously routed over)."
mplsTunnelMaxHops	" The maximum number of hops that can be specified for a tunnel on this device."
mplsTunnelName	" The canonical name assigned to the tunnel. This name can be used to refer to the tunnel on the LSR's console port. If mplsTunnelIsIf is set to true then the ifName of the interface corresponding to this tunnel should have a value equal to mplsTunnelName. Also see the description of ifName in RFC 2863." REFERENCE " RFC 2863 - The Interfaces Group MIB, McCloghrie, K., and F. Kastenholtz, June 2000"
mplsTunnelNotificationEnable	" If this object is true, then it enables the generation of mplsTunnelUp and mplsTunnelDown traps, otherwise these traps are not emitted."
mplsTunnelNotificationMaxRate	" This variable indicates the maximum number of notifications issued per second. If events occur more rapidly, the implementation may simply fail to emit these notifications during that period, or may queue them until an appropriate time. A value of 0 means no throttling is applied and events may be notified at the rate at which they occur."
mplsTunnelOperStatus	" Indicates the actual operational status of this tunnel, which is typically but not limited to, a function of the state of individual segments of this tunnel."

mplsTunnelOwner	" Denotes the entity that created and is responsible for managing this tunnel. This column is automatically filled by the agent on creation of a row."
mplsTunnelPathChanges	" Specifies the number of times the actual path for this tunnel instance has changed."
mplsTunnelPathInUse	" This value denotes the configured path that was chosen for this tunnel. This value reflects the secondary index into mplsTunnelHopTable. This path may not exactly match the one in mplsTunnelARHopTable due to the fact that some CSPF modification may have taken place. See mplsTunnelARHopTable for the actual path being taken by the tunnel. A value of zero denotes that no path is currently in use or available."
mplsTunnelPerfBytes	" Number of bytes forwarded by the tunnel. This object should represents the 32-bit value of the least significant part of the 64-bit value if both mplsTunnelPerfHCBytes is returned."
mplsTunnelPerfErrors	" Number of packets dropped because of errors or for other reasons."
mplsTunnelPerfHCBytes	" High capacity counter for number of bytes forwarded by the tunnel."
mplsTunnelPerfHCPackets	" High capacity counter for number of packets forwarded by the tunnel. "
mplsTunnelPerfPackets	" Number of packets forwarded by the tunnel. This object should represents the 32-bit value of the least significant part of the 64-bit value if both mplsTunnelPerfHCPackets is returned."
mplsTunnelPrimaryInstance	" Specifies the instance index of the primary instance of this tunnel. More details of the definition of tunnel instances and the primary tunnel instance can be found in the description of the TEXTUAL-CONVENTION MplsTunnelInstanceIndex."
mplsTunnelPrimaryUpTime	" Specifies the total time the primary instance of this tunnel has been active. The primary instance of this tunnel is defined in mplsTunnelPrimaryInstance."
mplsTunnelResourceExBurstSize	" The Excess burst size in bytes. The implementations which do not implement this variable must return noSuchObject exception for this object and must not allow a user to set this value." REFERENCE " CR-LDP Specification, Section 4.3."
mplsTunnelResourceFrequency	" The granularity of the availability of committed rate. The implementations which do not implement this variable must return unspecified(1) for this value and must not allow a user to set this value." REFERENCE " CR-LDP Specification, Section 4.3."

mplsTunnelResourceIndexNext	" This object contains the next appropriate value to be used for mplsTunnelResourceIndex when creating entries in the mplsTunnelResourceTable. If the number of unassigned entries is exhausted, a retrieval operation will return a value of 0. This object may also return a value of 0 when the LSR is unable to accept conceptual row creation, for example, if the mplsTunnelTable is implemented as read-only. To obtain the mplsTunnelResourceIndex value for a new entry, the manager must first issue a management protocol retrieval operation to obtain the current value of this object. When the SET is performed to create a row in the mplsTunnelResourceTable, the Command Responder (agent) must determine whether the value is indeed still unused; Two Network Management Applications may attempt to create a row (configuration entry) simultaneously and use the same value. If it is currently unused, the SET succeeds and the Command Responder (agent) changes the value of this object, according to an implementation-specific algorithm. If the value is in use, however, the SET fails. The Network Management Application must then re-read this variable to obtain a new usable value."
mplsTunnelResourceMaxBurstSize	" The maximum burst size in bytes."
mplsTunnelResourceMaxRate	" The maximum rate in bits/second. Note that setting mplsTunnelResourceMaxRate, mplsTunnelResourceMeanRate, and mplsTunnelResourceMaxBurstSize to 0 indicates best- effort treatment."
mplsTunnelResourceMeanBurstSize	" The mean burst size in bytes. The implementations which do not implement this variable must return a noSuchObject exception for this object and must not allow a user to set this object."
mplsTunnelResourceMeanRate	" This object is copied into an instance of mplsTrafficParamMeanRate in the mplsTrafficParamTable. The OID of this table entry is then copied into the corresponding mplsInSegmentTrafficParamPtr."
mplsTunnelResourcePointer	" This variable represents a pointer to the traffic parameter specification for this tunnel. This value may point at an entry in the mplsTunnelResourceEntry to indicate which mplsTunnelResourceEntry is to be assigned to this LSP instance. This value may optionally point at an externally defined traffic parameter specification table. A value of zeroDotZero indicates best-effort treatment. By having the same value of this object, two or more LSPs can indicate resource sharing."
mplsTunnelResourceRowStatus	" This variable is used to create, modify, and/or delete a row in this table. When a row in this table is in active(1) state, no objects in that row can be modified by the agent except mplsTunnelResourceRowStatus and mplsTunnelResourceStorageType."

mplsTunnelResourceStorageType	" The storage type for this Hop entry. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row."
mplsTunnelResourceWeight	" The relative weight for using excess bandwidth above its committed rate. The value of 0 means that weight is not applicable for the CR-LSP." REFERENCE " CR-LDP Specification, Section 4.3."
mplsTunnelRole	" This value signifies the role that this tunnel entry/instance represents. This value MUST be set to head(1) at the originating point of the tunnel. This value MUST be set to transit(2) at transit points along the tunnel, if transit points are supported. This value MUST be set to tail(3) at the terminating point of the tunnel if tunnel tails are supported. The value headTail(4) is provided for tunnels that begin and end on the same LSR."
mplsTunnelRowStatus	" This variable is used to create, modify, and/or delete a row in this table. When a row in this table is in active(1) state, no objects in that row can be modified by the agent except mplsTunnelAdminStatus, mplsTunnelRowStatus and mplsTunnelStorageType."
mplsTunnelSessionAttributes	" This bit mask indicates optional session values for this tunnel. The following describes these bit fields: fastRerouteThis flag indicates that the any tunnel hop may choose to reroute this tunnel without tearing it down. This flag permits transit routers to use a local repair mechanism which may result in violation of the explicit routing of this tunnel. When a fault is detected on an adjacent downstream link or node, a transit router can re-route traffic for fast service restoration. mergingPermitted This flag permits transit routers to merge this session with other RSVP sessions for the purpose of reducing resource overhead on downstream transit routers, thereby providing better network scaling. isPersistent Indicates whether this tunnel should be restored automatically after a failure occurs. isPinned This flag indicates whether the loose- routed hops of this tunnel are to be pinned. recordRouteThis flag indicates whether or not the signalling protocol should remember the tunnel path after it has been signaled." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001."
mplsTunnelSetupPrio	" Indicates the setup priority of this tunnel." REFERENCE " 1. RSVP-TE: Extensions to RSVP for LSP Tunnels, Awduche et al, RFC 3209, December 2001 2. Constraint-Based LSP Setup using LDP, Jamoussi (Editor), RFC 3212, January 2002"
mplsTunnelSignallingProto	" The signalling protocol, if any, used to setup this tunnel."
mplsTunnelStateTransitions	" Specifies the number of times the state (mplsTunnelOperStatus) of this tunnel instance has changed."

mplsTunnelStorageType	" The storage type for this tunnel entry. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row."
mplsTunnelTEDistProto	" The traffic engineering distribution protocol(s) used by this LSR. Note that an LSR may support more than one distribution protocol simultaneously."
mplsTunnelTotalUpTime	" This value represents the aggregate up time for all instances of this tunnel, if available. If this value is unavailable, it MUST return a value of 0."
mplsTunnelXCPointer	" This variable points to a row in the mplsXCTable. This table identifies the segments that compose this tunnel, their characteristics, and relationships to each other. A value of zeroDotZero indicates that no LSP has been associated with this tunnel yet." REFERENCE " Srinivasan, C., Viswanathan, A., and T. Nadeau, Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB), RFC 3813, June 2004"
mplsXCAdminStatus	" The desired operational status of this segment."
mplsXCIndexNext	" This object contains the next available value to be used for mplsXCIndex when creating entries in the mplsXCTable. A special value of the zero length string indicates that no more new entries can be created in the relevant table. Agents not allowing managers to create entries in this table MUST set this value to the zero length string."
mplsXCLabelStackIndex	" Primary index into mplsLabelStackTable identifying a stack of labels to be pushed beneath the top label. Note that the top label identified by the out- segment ensures that all the components of a multipoint-to-point connection have the same outgoing label. A value of the string containing the single octet 0x00 indicates that no labels are to be stacked beneath the top label. This object cannot be modified if mplsXCRowStatus is active(1)."
mplsXCLspId	" This value identifies the label switched path that this cross-connect entry belongs to. This object cannot be modified if mplsXCRowStatus is active(1) except for this object."
mplsXCNotificationsEnable	" If this object is set to true(1), then it enables the emission of mplsXCUp and mplsXCDown notifications; otherwise these notifications are not emitted." REFERENCE " See also RFC3413 for explanation that notifications are under the ultimate control of the MIB module in this document."
mplsXCOperStatus	" The actual operational status of this cross-connect."
mplsXCOwner	" Denotes the entity that created and is responsible for managing this cross-connect."
mplsXCRowStatus	" For creating, modifying, and deleting this row. When a row in this table has a row in the active(1) state, no objects in this row except this object and the mplsXCStorageType can be modified. "

mplsXCStorageType	" This variable indicates the storage type for this object. The agent MUST ensure that the associated in and out segments also have the same StorageType value and are restored consistently upon system restart. This value SHOULD be set to permanent(4) if created as a result of a static LSP configuration. Conceptual rows having the value 'permanent' need not allow write-access to any columnar objects in the row."

NOTIFICATION-LOG-MIB

The MIB module for logging SNMP Notifications, that is, Traps and Informs.

The following table lists the tables associated with this MIB:

MIB Name	Description
nlmConfigGlobalAgeOut	" The number of minutes a Notification SHOULD be kept in a log before it is automatically removed. If an application changes the value of nlmConfigGlobalAgeOut, Notifications older than the new time MAY be discarded to meet the new time. A value of 0 means no age out. Please be aware that contention between multiple managers trying to set this object to different values MAY affect the reliability and completeness of data seen by each manager."
nlmConfigGlobalEntryLimit	" The maximum number of notification entries that may be held in nlmLogTable for all nlmLogNames added together. A particular setting does not guarantee that much data can be held. If an application changes the limit while there are Notifications in the log, the oldest Notifications MUST be discarded to bring the log down to the new limit - thus the value of nlmConfigGlobalEntryLimit MUST take precedence over the values of nlmConfigGlobalAgeOut and nlmConfigLogEntryLimit, even if the Notification being discarded has been present for fewer minutes than the value of nlmConfigGlobalAgeOut, or if the named log has fewer entries than that specified in nlmConfigLogEntryLimit. A value of 0 means no limit. Please be aware that contention between multiple managers trying to set this object to different values MAY affect the reliability and completeness of data seen by each manager."
nlmStatsGlobalNotificationsBumped	" The number of log entries discarded to make room for a new entry due to lack of resources or the value of nlmConfigGlobalEntryLimit or nlmConfigLogEntryLimit. This does not include entries discarded due to the value of nlmConfigGlobalAgeOut."

nlmStatsGlobalNotificationsLogged	" The number of Notifications put into the nlmLogTable. This counts a Notification once for each log entry, so a Notification put into multiple logs is counted multiple times."

OSPF-MIB

The MIB module to describe the OSPF Version 2 Protocol.

The following table lists the tables associated with this MIB:

MIB Name	Description
ospfAddressLessIf	" For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address."
ospfAdminStat	" The administrative status of OSPF in the router. The value 'enabled' denotes that the OSPF Process is active on at least one interface; 'disabled' disables it on all interfaces. This object is persistent and when written the entity SHOULD save the change to non-volatile storage."
ospfAreaBdrRtrCount	" The total number of Area Border Routers reachable within this area. This is initially zero and is calculated in each Shortest Path First (SPF) pass."
ospfAreaBdrRtrStatus	" A flag to note whether this router is an Area Border Router." REFERENCE " OSPF Version 2, Section 3 Splitting the AS into Areas"
ospfAreaId	" A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone." REFERENCE " OSPF Version 2, Appendix C.2 Area parameters"
ospfAreaLsaCksumSum	" The 32-bit sum of the link state advertisements' LS checksums contained in this area's link state database. This sum excludes external (LS type-5) link state advertisements. The sum can be used to determine if there has been a change in a router's link state database, and to compare the link state database of two routers. The value should be treated as unsigned when comparing two sums of checksums."
ospfAreaLsaCount	" The total number of link state advertisements in this area's link state database, excluding AS-external LSAs."
ospfAreaLsaCountNumber	" Number of LSAs of a given type for a given area."
ospfAreaNssaTranslatorEvents	" Indicates the number of translator state changes that have occurred since the last boot-up. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at

	other times as indicated by the value of ospfDiscontinuityTime."
ospfAreaNssaTranslatorRole	" Indicates an NSSA border router's ability to perform NSSA translation of type-7 LSAs into type-5 LSAs."
ospfAreaNssaTranslatorStabilityInterval	" The number of seconds after an elected translator determines its services are no longer required, that it should continue to perform its translation duties."
ospfAreaNssaTranslatorState	" Indicates if and how an NSSA border router is performing NSSA translation of type-7 LSAs into type-5 LSAs. When this object is set to enabled, the NSSA Border router's OspfAreaNssaExtTranslatorRole has been set to always. When this object is set to elected, a candidate NSSA Border router is Translating type-7 LSAs into type-5. When this object is set to disabled, a candidate NSSA border router is NOT translating type-7 LSAs into type-5."
ospfAreaStatus	" This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified."
ospfAreaSummary	" The variable ospfAreaSummary controls the import of summary LSAs into stub and NSSA areas. It has no effect on other areas. If it is noAreaSummary, the router will not originate summary LSAs into the stub or NSSA area. It will rely entirely on its default route. If it is sendAreaSummary, the router will both summarize and propagate summary LSAs."
ospfAsBdrRtrCount	" The total number of Autonomous System Border Routers reachable within this area. This is initially zero and is calculated in each SPF pass."
ospfASBdrRtrStatus	" A flag to note whether this router is configured as an Autonomous System Border Router. This object is persistent and when written the entity SHOULD save the change to non-volatile storage." REFERENCE " OSPF Version 2, Section 3.3 Classification of routers"
ospfAsLsaCksumSum	" The 32-bit unsigned sum of the LS checksums of the AS link state advertisements contained in the AS-scope link state database. This sum can be used to determine if there has been a change in a router's AS-scope link state database, and to compare the AS-scope link state database of two routers."
ospfAsLsaCount	" The number of AS-scope link state advertisements in the AS-scope link state database."

ospfAsLsdbAdvertisement	" The entire link state advertisement, including its header." REFERENCE " OSPF Version 2, Section 12 Link State Advertisements. Note that for variable length LSAs, SNMP agents may not be able to return the largest string size."
ospfAsLsdbAge	" This field is the age of the link state advertisement in seconds." REFERENCE " OSPF Version 2, Section 12.1.1 LS age"
ospfAsLsdbChecksum	" This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum." REFERENCE " OSPF Version 2, Section 12.1.7 LS checksum"
ospfAsLsdbSequence	" The sequence number field is a signed 32-bit integer. It starts with the value '80000001'h, or -'7FFFFFFF'h, and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number, the more recent the advertisement." REFERENCE " OSPF Version 2, Section 12.1.6 LS sequence number"
ospfDemandExtensions	" The router's support for demand routing. This object is persistent and when written the entity SHOULD save the change to non-volatile storage." REFERENCE " Extending OSPF to Support Demand Circuits"
ospfDiscontinuityTime	" The value of sysUpTime on the most recent occasion at which any one of this MIB's counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value."
ospfExitOverflowInterval	" The number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState. This allows the router to again originate non-default AS-external LSAs. When set to 0, the router will not leave overflow state until restarted. This object is persistent and when written the entity SHOULD save the change to non-volatile storage."
ospfExternLsaCksumSum	" The 32-bit sum of the LS checksums of the external link state advertisements contained in the link state database. This sum can be used to determine if there has been a change in a router's link state database and to compare the link state database of two routers. The value should be treated as unsigned when comparing two sums of checksums."

ospfExternLsaCount	" The number of external (LS type-5) link state advertisements in the link state database." REFERENCE " OSPF Version 2, Appendix A.4.5 AS external link advertisements"
ospfExtLsdbAdvertisement	" The entire link state advertisement, including its header." REFERENCE " OSPF Version 2, Section 12 Link State Advertisements"
ospfExtLsdbAge	" This field is the age of the link state advertisement in seconds." REFERENCE " OSPF Version 2, Section 12.1.1 LS age"
ospfExtLsdbChecksum	" This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum." REFERENCE " OSPF Version 2, Section 12.1.7 LS checksum"
ospfExtLsdbLimit	" The maximum number of non-default AS-external LSAs entries that can be stored in the link state database. If the value is -1, then there is no limit. When the number of non-default AS-external LSAs in a router's link state database reaches ospfExtLsdbLimit, the router enters overflow state. The router never holds more than ospfExtLsdbLimit non-default AS-external LSAs in its database. OspfExtLsdbLimit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area (i.e., OSPF stub areas and NSSAs are excluded). This object is persistent and when written the entity SHOULD save the change to non-volatile storage."
ospfExtLsdbLsid	" The Link State ID is an LS Type Specific field containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement." REFERENCE " OSPF Version 2, Section 12.1.4 Link State ID"
ospfExtLsdbRouterId	" The 32-bit number that uniquely identifies the originating router in the Autonomous System." REFERENCE " OSPF Version 2, Appendix C.1 Global parameters"
ospfExtLsdbSequence	" The sequence number field is a signed 32-bit integer. It starts with the value '80000001'h, or -'7FFFFFFF'h, and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative. It is used to detect old and duplicate link state advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number, the more recent the advertisement." REFERENCE " OSPF Version 2, Section 12.1.6 LS sequence number"
ospfExtLsdbType	" The type of the link state advertisement. Each link state type has a separate advertisement format." REFERENCE " OSPF Version 2, Appendix A.4.1 The Link State Advertisement header"

ospfHostAreaID	" The OSPF area to which the host belongs. Deprecated by ospfHostCfgAreaID." REFERENCE " OSPF Version 2, Appendix C.7 Host parameters"
ospfHostCfgAreaID	" To configure the OSPF area to which the host belongs." REFERENCE " OSPF Version 2, Appendix C.7 Host parameters"
ospfHostIpAddress	" The IP address of the host." REFERENCE " OSPF Version 2, Appendix C.7 Host route parameters"
ospfHostMetric	" The metric to be advertised." REFERENCE " OSPF Version 2, Appendix C.7 Host route parameters"
ospfHostStatus	" This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified."
ospfHostTOS	" The Type of Service of the route being configured." REFERENCE " OSPF Version 2, Appendix C.7 Host route parameters"
ospfIfAdminStat	" The OSPF interface's administrative status. The value formed on the interface, and the interface will be advertised as an internal route to some area. The value 'disabled' denotes that the interface is external to OSPF."
ospfIfAreaId	" A 32-bit integer uniquely identifying the area to which the interface connects. Area ID 0.0.0.0 is used for the OSPF backbone."
ospfIfAuthType	" The authentication type specified for an interface. Note that this object can be used to engage in significant attacks against an OSPF router." REFERENCE " OSPF Version 2, Appendix D Authentication"
ospfIfBackupDesignatedRouter	" The IP address of the backup designated router."
ospfIfBackupDesignatedRouterId	" The Router ID of the backup designated router."
ospfIfDemand	" Indicates whether Demand OSPF procedures (hello suppression to FULL neighbors and setting the DoNotAge flag on propagated LSAs) should be performed on this interface."
ospfIfDesignatedRouter	" The IP address of the designated router."
ospfIfDesignatedRouterId	" The Router ID of the designated router."
ospfIfEvents	" The number of times this OSPF interface has changed its state or an error has occurred. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ospfDiscontinuityTime."
ospfIfHelloInterval	" The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network."
ospfIfIpAddress	" The IP address of this OSPF interface."

ospfIfLsaCksumSum	"The 32-bit unsigned sum of the Link State Advertisements' LS checksums contained in this interface's link-local link state database. The sum can be used to determine if there has been a change in the interface's link state database and to compare the interface link state database of routers attached to the same subnet."
ospfIfLsaCount	"The total number of link-local link state advertisements in this interface's link-local link state database."
ospfIfMetricAddressLessIf	"For the purpose of easing the instancing of addressed and addressless interfaces; this variable takes the value 0 on interfaces with IP addresses and the value of ifIndex for interfaces having no IP address. On row creation, this can be derived from the instance."
ospfIfMetricIpAddress	"The IP address of this OSPF interface. On row creation, this can be derived from the instance."
ospfIfMetricStatus	"This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified."
ospfIfMetricTOS	"The Type of Service metric being referenced. On row creation, this can be derived from the instance."
ospfIfMetricValue	"The metric of using this Type of Service on this interface. The default value of the TOS 0 metric is 10^8 / ifSpeed."
ospfIfMulticastForwarding	"The way multicasts should be forwarded on this interface: not forwarded, forwarded as data link multicasts, or forwarded as data link unicasts. Data link multicasting is not meaningful on point-to-point and NBMA interfaces, and setting ospfMulticastForwarding to 0 effectively disables all multicast forwarding."
ospfIfPollInterval	"The larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor."
ospfIfRetransInterval	"The number of seconds between link state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and Link State request packets. Note that minimal value SHOULD be 1 second."
ospfIfRtrDeadInterval	"The number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network."
ospfIfRtrPriority	"The priority of this interface. Used in multi-access networks, this field is used in the designated router election algorithm. The value 0 signifies that the router is not eligible to become the designated router on this particular network. In the event of a tie in this value, routers will use their Router ID as a tie breaker."

ospfIfState	" The OSPF Interface State."
ospfIfStatus	" This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified."
ospfIfTransitDelay	" The estimated number of seconds it takes to transmit a link state update packet over this interface. Note that the minimal value SHOULD be 1 second."
ospfIfType	" The OSPF interface type. By way of a default, this field may be intuited from the corresponding value of ifType. Broadcast LANs, such as Ethernet and IEEE 802.5, take the value 'broadcast', X.25 and similar technologies take the value 'nbma', and links that are definitively point to point take the value 'pointToPoint'."
ospfImportAsExtern	" Indicates if an area is a stub area, NSSA, or standard area. Type-5 AS-external LSAs and type-11 Opaque LSAs are not imported into stub areas or NSSAs. NSSAs import AS-external data as type-7 LSAs" REFERENCE " OSPF Version 2, Appendix C.2 Area parameters"
ospfLsdbAdvertisement	" The entire link state advertisement, including its header. Note that for variable length LSAs, SNMP agents may not be able to return the largest string size." REFERENCE " OSPF Version 2, Section 12 Link State Advertisements"
ospfLsdbAge	" This field is the age of the link state advertisement in seconds." REFERENCE " OSPF Version 2, Section 12.1.1 LS age"
ospfLsdbAreaId	" The 32-bit identifier of the area from which the LSA was received." REFERENCE " OSPF Version 2, Appendix C.2 Area parameters"
ospfLsdbChecksum	" This field is the checksum of the complete contents of the advertisement, excepting the age field. The age field is excepted so that an advertisement's age can be incremented without updating the checksum. The checksum used is the same that is used for ISO connectionless datagrams; it is commonly referred to as the Fletcher checksum." REFERENCE " OSPF Version 2, Section 12.1.7 LS checksum"
ospfLsdbLsid	" The Link State ID is an LS Type Specific field containing either a Router ID or an IP address; it identifies the piece of the routing domain that is being described by the advertisement." REFERENCE " OSPF Version 2, Section 12.1.4 Link State ID"
ospfLsdbRouterId	" The 32-bit number that uniquely identifies the originating router in the Autonomous System." REFERENCE " OSPF Version 2, Appendix C.1 Global parameters"

ospfLsdbSequence	" The sequence number field is a signed 32-bit integer. It starts with the value '80000001'h, or -'7FFFFFFF'h, and increments until '7FFFFFFF'h. Thus, a typical sequence number will be very negative. It is used to detect old and duplicate Link State Advertisements. The space of sequence numbers is linearly ordered. The larger the sequence number, the more recent the advertisement." REFERENCE " OSPF Version 2, Section 12.1.6 LS sequence number"
ospfLsdbType	" The type of the link state advertisement. Each link state type has a separate advertisement format. Note: External link state advertisements are permitted for backward compatibility, but should be displayed in the ospfAsLsdbTable rather than here." REFERENCE " OSPF Version 2, Appendix A.4.1 The Link State Advertisement header"
ospfMulticastExtensions	" A bit mask indicating whether the router is forwarding IP multicast (Class D) datagrams based on the algorithms defined in the multicast extensions to OSPF. Bit 0, if set, indicates that the router can forward IP multicast datagrams in the router's directly attached areas (called intra-area multicast routing). Bit 1, if set, indicates that the router can forward IP multicast datagrams between OSPF areas (called inter-area multicast routing). Bit 2, if set, indicates that the router can forward IP multicast datagrams between Autonomous Systems (called inter-AS multicast routing). Only certain combinations of bit settings are allowed, namely: 0 (no multicast forwarding is enabled), 1 (intra-area multicasting only), 3 (intra-area and inter-area multicasting), 5 (intra-area and inter-AS multicasting), and 7 (multicasting everywhere). By default, no multicast forwarding is enabled. This object is persistent and when written the entity SHOULD save the change to non-volatile storage."
ospfNbmaNbrPermanence	" This variable displays the status of the entry; 'dynamic' and 'permanent' refer to how the neighbor became known."
ospfNbmaNbrStatus	" This object permits management of the table by facilitating actions such as row creation, construction, and destruction. The value of this object has no effect on whether other objects in this conceptual row can be modified."
ospfNbrAddressLessIndex	" On an interface having an IP address, zero. On addressless interfaces, the corresponding value of ifIndex in the Internet Standard MIB. On row creation, this can be derived from the instance."
ospfNbrEvents	" The number of times this neighbor relationship has changed state or an error has occurred. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ospfDiscontinuityTime."

ospfNbrHelloSuppressed	" Indicates whether Hellos are being suppressed to the neighbor."
ospfNbrIpAddr	" The IP address this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0 but the address of another of the neighbor's interfaces."
ospfNbrLsRetransQLen	" The current length of the retransmission queue."
ospfNbrOptions	" A bit mask corresponding to the neighbor's options field. Bit 0, if set, indicates that the system will operate on Type of Service metrics other than TOS 0. If zero, the neighbor will ignore all metrics except the TOS 0 metric. Bit 1, if set, indicates that the associated area accepts and operates on external information; if zero, it is a stub area. Bit 2, if set, indicates that the system is capable of routing IP multicast datagrams, that is that it implements the multicast extensions to OSPF. Bit 3, if set, indicates that the associated area is an NSSA. These areas are capable of carrying type-7 external advertisements, which are translated into type-5 external advertisements at NSSA borders." REFERENCE " OSPF Version 2, Section 12.1.2 Options"
ospfNbrPriority	" The priority of this neighbor in the designated router election algorithm. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network."
ospfNbrRestartHelperAge	" Remaining time in current OSPF graceful restart interval, if the router is acting as a restart helper for the neighbor."
ospfNbrRestartHelperExitReason	" Describes the outcome of the last attempt at acting as a graceful restart helper for the neighbor."
ospfNbrRestartHelperStatus	" Indicates whether the router is acting as a graceful restart helper for the neighbor."
ospfNbrRtrId	" A 32-bit integer (represented as a type IpAddress) uniquely identifying the neighboring router in the Autonomous System."
ospfNbrState	" The state of the relationship with this neighbor." REFERENCE " OSPF Version 2, Section 10.1 Neighbor States"
ospfOpaqueLsaSupport	" The router's support for Opaque LSA types." REFERENCE " The OSPF Opaque LSA Option"
ospfOriginateNewLsas	" The number of new link state advertisements that have been originated. This number is incremented each time the router originates a new LSA. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ospfDiscontinuityTime."
ospfSpfRuns	" The number of times that the intra-area route table has been calculated using this area's link state database. This is typically done using Dijkstra's algorithm. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ospfDiscontinuityTime."

ospfStubRouterAdvertisement	" This object controls the advertisement of stub router LSAs by the router. The value doNotAdvertise will result in the advertisement of a standard router LSA and is the default value. This object is persistent and when written the entity SHOULD save the change to non-volatile storage."
ospfStubRouterSupport	" The router's support for stub router functionality." REFERENCE " OSPF Stub Router Advertisement"
ospfTOSSupport	" The router's support for type-of-service routing. This object is persistent and when written the entity SHOULD save the change to non-volatile storage." REFERENCE " OSPF Version 2, Appendix F.1.2 Optional TOS support"
ospfVersionNumber	" The current version number of the OSPF protocol is 2." REFERENCE " OSPF Version 2, Title"

OSPF-TRAP-MIB

The MIB module to describe traps for the OSPF Version 2 Protocol.

The following table lists the tables associated with this MIB:

MIB Name	Description
ospfConfigErrorType	" Potential types of configuration conflicts. Used by the ospfConfigError and ospfConfigVirtError traps. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as noError."
ospfPacketSrc	" The IP address of an inbound packet that cannot be identified by a neighbor instance. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as 0.0.0.0."
ospfPacketType	" OSPF packet types. When the last value of a trap using this object is needed, but no traps of that type have been sent, this value pertaining to this object should be returned as nullPacket."

ospfSetTrap	" A 4-octet string serving as a bit map for the trap events defined by the OSPF traps. This object is used to enable and disable specific OSPF traps where a 1 in the bit field represents enabled. The right-most bit (least significant) represents trap 0. This object is persistent and when written the entity SHOULD save the change to non-volatile storage."

RSVP-MIB

The MIB module to describe the RSVP Protocol"

The following table lists the tables associated with this MIB:

MIB Name	Description
rsvpIfEnabled	" If TRUE, RSVP is enabled on this Interface. If FALSE, RSVP is not enabled on this interface."
rsvpIfIpNbrs	" The number of neighbors perceived to be using only the RSVP IP Encapsulation."
rsvpIfNbrs	" The number of neighbors currently perceived; this will exceed rsvpIfIpNbrs + rsvpIfUdpNbrs by the number of neighbors using both encapsulations."
rsvpIfRefreshBlockadeMultiple	" The value of the RSVP value 'Kb', Which is the minimum number of refresh intervals that blockade state will last once entered."
rsvpIfRefreshInterval	" The value of the RSVP value 'R', which is the minimum period between refresh transmissions of a given PATH or RESV message on an interface." -- 30 seconds
rsvpIfRefreshMultiple	" The value of the RSVP value 'K', which is the number of refresh intervals which must elapse (minimum) before a PATH or RESV message which is not being refreshed will be aged out."
rsvpIfRouteDelay	" The approximate period from the time a route is changed to the time a resulting message appears on the interface."
rsvpIfStatus	" 'active' on interfaces that are configured for RSVP."
rsvpIfTTL	" The value of SEND_TTL used on this interface for messages this node originates. If set to zero, the node determines the TTL via other means."
rsvpIfUdpNbrs	" The number of neighbors perceived to be using only the RSVP UDP Encapsulation."
rsvpIfUdpRequired	" If TRUE, manual configuration forces the use of UDP encapsulation on the interface. If FALSE, UDP encapsulation is only used if rsvpIfUdpNbrs is not zero."
rsvpNbrProtocol	" The encapsulation being used by this neighbor."

rsvpNbrStatus	" 'active' for all neighbors. This object may be used to configure neighbors. In the presence of configured neighbors, the implementation may (but is not required to) limit the set of valid neighbors to those configured."
rsvpResvDestAddr	" The destination address used by all senders in this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvDestAddrLength	" The length of the destination address in bits. This is the CIDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvDestPort	" The UDP or TCP port number used as a destination port for all senders in this session. If the IP protocol in use, specified by rsvpResvProtocol, is 50 (ESP) or 51 (AH), this represents a virtual destination port number. A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvExplicit	" If TRUE, individual senders are listed using Filter Specifications. If FALSE, all senders are implicitly selected. The Scope Object will contain a list of senders that need to receive this reservation request for the purpose of routing the RESV message."
rsvpResvFlowId	" The flow ID that this receiver is using, if this is an IPv6 session."
rsvpResvFwdDestAddr	" The destination address used by all senders in this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdDestAddrLength	" The length of the destination address in bits. This is the CIDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdDestPort	" The UDP or TCP port number used as a destination port for all senders in this session. If the IP protocol in use, specified by rsvpResvFwdProtocol, is 50 (ESP) or 51 (AH), this represents a virtual destination port number. A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdExplicit	" If TRUE, individual senders are listed using Filter Specifications. If FALSE, all senders are implicitly selected. The Scope Object will contain a list of senders that need to receive this reservation request for the purpose of routing the RESV message."
rsvpResvFwdFlowId	" The flow ID that this receiver is using, if this is an IPv6 session."
rsvpResvFwdHopAddr	" The address of the (previous) RSVP that will receive this message."

rsvpResvFwdHopLih	" The Logical Interface Handle sent to the (previous) RSVP that will receive this message."
rsvpResvFwdInterface	" The ifIndex value of the interface on which this RESV message was most recently sent."
rsvpResvFwdInterval	" The interval between refresh messages advertised to the Previous Hop."
rsvpResvFwdLastChange	" The time of the last change in this request; This is either the first time it was sent or the time of the most recent change in parameters."
rsvpResvFwdPolicy	" The contents of the policy object, displayed as an uninterpreted string of octets, including the object header. In the absence of such an object, this should be of zero length."
rsvpResvFwdPort	" The UDP or TCP port number used as a source port for this sender in this session. If the IP protocol in use, specified by rsvpResvFwdProtocol is 50 (ESP) or 51 (AH), this represents a generalized port identifier (GPI). A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdProtocol	" The IP Protocol used by a session. for secure sessions, this indicates IP Security. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdRSpecRate	" If the requested service is Guaranteed, as specified by rsvpResvService, this is the clearing rate that is being requested. Otherwise, it is zero, or the agent may return noSuchValue."
rsvpResvFwdRSpecSlack	" If the requested service is Guaranteed, as specified by rsvpResvService, this is the delay slack. Otherwise, it is zero, or the agent may return noSuchValue."
rsvpResvFwdRSVPHop	" If TRUE, the node believes that the next IP hop is an RSVP hop. If FALSE, the node believes that the next IP hop may not be an RSVP hop."
rsvpResvFwdScope	" The contents of the scope object, displayed as an uninterpreted string of octets, including the object header. In the absence of such an object, this should be of zero length."
rsvpResvFwdSenderAddr	" The source address of the sender selected by this reservation. The value of all zeroes indicates 'all senders'. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdSenderAddrLength	" The length of the sender's address in bits. This is the ClDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvFwdService	" The QoS Service classification requested."
rsvpResvFwdShared	" If TRUE, a reservation shared among senders is requested. If FALSE, a reservation specific to this sender is requested."

rsvpResvFwdStatus	" 'active' for all active RESV messages. This object may be used to delete RESV information."
rsvpResvFwdTSpecBurst	" The size of the largest burst expected from the sender at a time. If this is less than the sender's advertised burst size, the receiver is asking the network to provide flow pacing beyond what would be provided under normal circumstances. Such pacing is at the network's option."
rsvpResvFwdTSpecMaxTU	" The maximum message size for this flow. The admission algorithm will reject TSpecs whose Maximum Transmission Unit, plus the interface headers, exceed the interface MTU."
rsvpResvFwdTSpecMinTU	" The minimum message size for this flow. The policing algorithm will treat smaller messages as though they are this size."
rsvpResvFwdTSpecPeakRate	" The Peak Bit Rate of the sender's data stream Traffic arrival is not expected to exceed this rate at any time, apart from the effects of jitter in the network. If not specified in the TSpec, this returns zero or noSuchValue."
rsvpResvFwdTSpecRate	" The Average Bit Rate of the sender's data stream. Within a transmission burst, the arrival rate may be as fast as rsvpResvFwdTSpecPeakRate (if supported by the service model); however, averaged across two or more burst intervals, the rate should not exceed rsvpResvFwdTSpecRate. Note that this is a prediction, often based on the general capability of a type of codec or particular encoding; the measured average rate may be significantly lower."
rsvpResvFwdTTL	" The TTL value in the RSVP header that was last received."
rsvpResvFwdType	" The type of session (IP4, IP6, IP6 with flow information, etc)."
rsvpResvHopAddr	" The address used by the next RSVP hop (which may be the ultimate receiver)."
rsvpResvHopLih	" The Logical Interface Handle received from the previous RSVP hop (which may be the ultimate receiver)."
rsvpResvInterface	" The ifIndex value of the interface on which this RESV message was most recently received."
rsvpResvInterval	" The interval between refresh messages as advertised by the Next Hop."
rsvpResvLastChange	" The time of the last change in this reservation request; This is either the first time it was received or the time of the most recent change in parameters."
rsvpResvPolicy	" The contents of the policy object, displayed as an uninterpreted string of octets, including the object header. In the absence of such an object, this should be of zero length."

rsvpResvPort	" The UDP or TCP port number used as a source port for this sender in this session. If the IP protocol in use, specified by rsvpResvProtocol is 50 (ESP) or 51 (AH), this represents a generalized port identifier (GPI). A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvProtocol	" The IP Protocol used by this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvRSpecRate	" If the requested service is Guaranteed, as specified by rsvpResvService, this is the clearing rate that is being requested. Otherwise, it is zero, or the agent may return noSuchValue."
rsvpResvRSpecSlack	" If the requested service is Guaranteed, as specified by rsvpResvService, this is the delay slack. Otherwise, it is zero, or the agent may return noSuchValue."
rsvpResvRSVPHop	" If TRUE, the node believes that the previous IP hop is an RSVP hop. If FALSE, the node believes that the previous IP hop may not be an RSVP hop."
rsvpResvScope	" The contents of the scope object, displayed as an uninterpreted string of octets, including the object header. In the absence of such an object, this should be of zero length. If the length is non-zero, this contains a series of IP4 or IP6 addresses."
rsvpResvSenderAddr	" The source address of the sender selected by this reservation. The value of all zeroes indicates 'all senders'. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvSenderAddrLength	" The length of the sender's address in bits. This is the CIDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpResvService	" The QoS Service classification requested by the receiver."
rsvpResvShared	" If TRUE, a reservation shared among senders is requested. If FALSE, a reservation specific to this sender is requested."
rsvpResvStatus	" 'active' for all active RESV messages. This object may be used to install static RESV information or delete RESV information."
rsvpResvTSpecBurst	" The size of the largest burst expected from the sender at a time. If this is less than the sender's advertised burst size, the receiver is asking the network to provide flow pacing beyond what would be provided under normal circumstances. Such pacing is at the network's option."
rsvpResvTSpecMaxTU	" The maximum message size for this flow. The admission algorithm will reject TSpecs whose Maximum Transmission Unit, plus the interface headers, exceed the interface MTU."

rsvpResvTSpecMinTU	" The minimum message size for this flow. The policing algorithm will treat smaller messages as though they are this size."
rsvpResvTSpecPeakRate	" The Peak Bit Rate of the sender's data stream. Traffic arrival is not expected to exceed this rate at any time, apart from the effects of jitter in the network. If not specified in the TSpec, this returns zero or noSuchValue."
rsvpResvTSpecRate	" The Average Bit Rate of the sender's data stream. Within a transmission burst, the arrival rate may be as fast as rsvpResvTSpecPeakRate (if supported by the service model); however, averaged across two or more burst intervals, the rate should not exceed rsvpResvTSpecRate. Note that this is a prediction, often based on the general capability of a type of codec or particular encoding; the measured average rate may be significantly lower."
rsvpResvTTL	" The TTL value in the RSVP header that was last received."
rsvpResvType	" The type of session (IP4, IP6, IP6 with flow information, etc)."
rsvpSenderAddr	" The source address used by this sender in this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderAddrLength	" The length of the sender's address in bits. This is the CIDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderAdspecBreak	" The global break bit general characterization parameter from the ADSPEC. If TRUE, at least one non-IS hop was detected in the path. If FALSE, no non-IS hops were detected."
rsvpSenderAdspecCtrlLoadBreak	" If TRUE, the Controlled Load Service fragment has its 'break' bit set, indicating that one or more nodes along the path do not support the controlled load service. If FALSE, and rsvpSenderAdspecCtrlLoadSvc is TRUE, the 'break' bit is not set. If rsvpSenderAdspecCtrlLoadSvc is FALSE, this returns FALSE or noSuchValue."
rsvpSenderAdspecCtrlLoadHopCount	" If rsvpSenderAdspecCtrlLoadSvc is TRUE, this is the service-specific override of the hop count general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecCtrlLoadSvc is FALSE, this returns zero or noSuchValue."

rsvpSenderAdspecCtrlLoadMinLatency	" If rsvpSenderAdspecCtrlLoadSvc is TRUE, this is the service-specific override of the minimum path latency general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecCtrlLoadSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecCtrlLoadMtu	" If rsvpSenderAdspecCtrlLoadSvc is TRUE, this is the service-specific override of the composed Maximum Transmission Unit general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecCtrlLoadSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecCtrlLoadPathBw	" If rsvpSenderAdspecCtrlLoadSvc is TRUE, this is the service-specific override of the path bandwidth estimate general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecCtrlLoadSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecCtrlLoadSvc	" If TRUE, the ADSPEC contains a Controlled Load Service fragment. If FALSE, the ADSPEC does not contain a Controlled Load Service fragment."
rsvpSenderAdspecGuaranteedBreak	" If TRUE, the Guaranteed Service fragment has its 'break' bit set, indicating that one or more nodes along the path do not support the guaranteed service. If FALSE, and rsvpSenderAdspecGuaranteedSvc is TRUE, the 'break' bit is not set. If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns FALSE or noSuchValue."
rsvpSenderAdspecGuaranteedCsum	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the composed value for the guaranteed service 'C' parameter since the last reshaping point. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedCtot	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the end-to-end composed value for the guaranteed service 'C' parameter. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."

rsvpSenderAdspecGuaranteedDsum	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the composed value for the guaranteed service 'D' parameter since the last reshaping point. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedDtot	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the end-to-end composed value for the guaranteed service 'D' parameter. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedHopCount	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the service-specific override of the hop count general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedMinLatency	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the service-specific override of the minimum path latency general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedMtu	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the service-specific override of the composed Maximum Transmission Unit general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedPathBw	" If rsvpSenderAdspecGuaranteedSvc is TRUE, this is the service-specific override of the path bandwidth estimate general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present If rsvpSenderAdspecGuaranteedSvc is FALSE, this returns zero or noSuchValue."
rsvpSenderAdspecGuaranteedSvc	" If TRUE, the ADSPEC contains a Guaranteed Service fragment. If FALSE, the ADSPEC does not contain a Guaranteed Service fragment."

rsvpSenderAdspecHopCount	" The hop count general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present"
rsvpSenderAdspecMinLatency	" The minimum path latency general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present"
rsvpSenderAdspecMtu	" The composed Maximum Transmission Unit general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present"
rsvpSenderAdspecPathBw	" The path bandwidth estimate general characterization parameter from the ADSPEC. A return of zero or noSuchValue indicates one of the following conditions: the invalid bit was set the parameter was not present"
rsvpSenderDestAddr	" The destination address used by all senders in this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderDestAddrLength	" The length of the destination address in bits. This is the CIDR Prefix Length, which for IP4 hosts and multicast addresses is 32 bits. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderDestPort	" The UDP or TCP port number used as a destination port for all senders in this session. If the IP protocol in use, specified by rsvpSenderProtocol, is 50 (ESP) or 51 (AH), this represents a virtual destination port number. A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderFlowId	" The flow ID that this sender is using, if this is an IPv6 session."
rsvpSenderHopAddr	" The address used by the previous RSVP hop (which may be the original sender)."
rsvpSenderHopLih	" The Logical Interface Handle used by the previous RSVP hop (which may be the original sender)."
rsvpSenderInterface	" The ifIndex value of the interface on which this PATH message was most recently received."
rsvpSenderInterval	" The interval between refresh messages as advertised by the Previous Hop."
rsvpSenderLastChange	" The time of the last change in this PATH message; This is either the first time it was received or the time of the most recent change in parameters."
rsvpSenderOutInterfaceStatus	" 'active' for all active PATH messages."

rsvpSenderPolicy	" The contents of the policy object, displayed as an uninterpreted string of octets, including the object header. In the absence of such an object, this should be of zero length."
rsvpSenderPort	" The UDP or TCP port number used as a source port for this sender in this session. If the IP protocol in use, specified by rsvpSenderProtocol is 50 (ESP) or 51 (AH), this represents a generalized port identifier (GPI). A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderProtocol	" The IP Protocol used by this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSenderRSVPHop	" If TRUE, the node believes that the previous IP hop is an RSVP hop. If FALSE, the node believes that the previous IP hop may not be an RSVP hop."
rsvpSenderStatus	" 'active' for all active PATH messages. This object may be used to install static PATH information or delete PATH information."
rsvpSenderTSpecBurst	" The size of the largest burst expected from the sender at a time."
rsvpSenderTSpecMaxTU	" The maximum message size for this flow. The admission algorithm will reject TSpecs whose Maximum Transmission Unit, plus the interface headers, exceed the interface MTU."
rsvpSenderTSpecMinTU	" The minimum message size for this flow. The policing algorithm will treat smaller messages as though they are this size."
rsvpSenderTSpecPeakRate	" The Peak Bit Rate of the sender's data stream. Traffic arrival is not expected to exceed this rate at any time, apart from the effects of jitter in the network. If not specified in the TSpec, this returns zero or noSuchValue."
rsvpSenderTSpecRate	" The Average Bit Rate of the sender's data stream. Within a transmission burst, the arrival rate may be as fast as rsvpSenderTSpecPeakRate (if supported by the service model); however, averaged across two or more burst intervals, the rate should not exceed rsvpSenderTSpecRate. Note that this is a prediction, often based on the general capability of a type of codec or particular encoding; the measured average rate may be significantly lower."
rsvpSenderTTL	" The TTL value in the RSVP header that was last received."
rsvpSenderType	" The type of session (IP4, IP6, IP6 with flow information, etc)."
rsvpSessionDestAddr	" The destination address used by all senders in this session. This object may not be changed when the value of the RowStatus object is 'active'."

rsvpSessionDestAddrLength	" The CIDR prefix length of the session address, which is 32 for IP4 host and multicast addresses, and 128 for IP6 addresses. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSessionPort	" The UDP or TCP port number used as a destination port for all senders in this session. If the IP protocol in use, specified by rsvpSenderProtocol, is 50 (ESP) or 51 (AH), this represents a virtual destination port number. A value of zero indicates that the IP protocol in use does not have ports. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSessionProtocol	" The IP Protocol used by this session. This object may not be changed when the value of the RowStatus object is 'active'."
rsvpSessionReceivers	" The number of reservations being requested of this system for this session."
rsvpSessionRequests	" The number of reservation requests this system is sending upstream for this session."
rsvpSessionSenders	" The number of distinct senders currently known to be part of this session."
rsvpSessionType	" The type of session (IP4, IP6, IP6 with flow information, etc)."

SNMPv2-MIB

The MIB module for SNMP entities.

The following table lists the tables associated with this MIB:

MIB Name	Description
snmpEnableAuthenTraps	" Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled. Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system."
snmpInASNParseErrs	" The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages."

snmpInBadCommunityNames	" The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which used an SNMP community name not known to said entity. Also, implementations which authenticate community-based SNMP messages using check(s) in addition to matching the community name (for example, by also checking whether the message originated from a transport address allowed to use a specified community name) MAY include in this value the number of messages which failed the additional check(s). It is strongly RECOMMENDED that the documentation for any security model which is used to authenticate community-based SNMP messages specify the precise conditions that contribute to this value."
snmpInBadCommunityUses	" The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which represented an SNMP operation that was not allowed for the SNMP community named in the message. The precise conditions under which this counter is incremented (if at all) depend on how the SNMP entity implements its access control mechanism and how its applications interact with that access control mechanism. It is strongly RECOMMENDED that the documentation for any access control mechanism which is used to control access to and visibility of MIB instrumentation specify the precise conditions that contribute to this value."
snmpInBadValues	" The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `badValue'."
snmpInBadVersions	" The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version."
snmpInGenErrs	" The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `genErr'."
snmpInGetNexts	" The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity."
snmpInGetRequests	" The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity."
snmpInGetResponses	" The total number of SNMP Get-Response PDUs which have been accepted and processed by the SNMP protocol entity."
snmpInNoSuchNames	" The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `noSuchName'."
snmpInPkts	" The total number of messages delivered to the SNMP entity from the transport service."

snmpInReadOnlys	" The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `readOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value `readOnly' in the error-status field, as such this object is provided as a means of detecting incorrect implementations of the SNMP."
snmpInSetRequests	" The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity."
snmpInTooBigs	" The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field was `tooBig'."
snmpInTotalReqVars	" The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs."
snmpInTotalSetVars	" The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs."
snmpInTraps	" The total number of SNMP Trap PDUs which have been accepted and processed by the SNMP protocol entity."
snmpOutBadValues	" The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `badValue'."
snmpOutGenErrs	" The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `genErr'."
snmpOutGetNexts	" The total number of SNMP Get-Next PDUs which have been generated by the SNMP protocol entity."
snmpOutGetRequests	" The total number of SNMP Get-Request PDUs which have been generated by the SNMP protocol entity."
snmpOutGetResponses	" The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity."
snmpOutNoSuchNames	" The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status was `noSuchName'."
snmpOutPkts	" The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service."
snmpOutSetRequests	" The total number of SNMP Set-Request PDUs which have been generated by the SNMP protocol entity."
snmpOutTooBigs	" The total number of SNMP PDUs which were generated by the SNMP protocol entity and for which the value of the error-status field was `tooBig.'"

snmpOutTraps	" The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity."
snmpProxyDrops	" The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDU (such as a Response-PDU) could be returned."
snmpSetSerialNo	" An advisory lock used to allow several cooperating command generator applications to coordinate their use of the SNMP set operation. This object is used for coarse-grain coordination. To achieve fine-grain coordination, one or more similar objects might be defined within each MIB group, as appropriate."
snmpSilentDrops	" The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDU (such as a Response-PDU) with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request."
sysContact	" The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string."
sysDescr	" A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software."
sysLocation	" The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is the zero-length string."
sysName	" An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string."
sysObjectID	" The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor `Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.424242, it could assign the identifier 1.3.6.1.4.1.424242.1.1 to its `Fred Router'."

sysServices	" A value which indicates the set of services that this entity may potentially offer. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). Note that in the context of the Internet suite of protocols, values should be calculated accordingly: layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., supports the IP) 4 end-to-end (e.g., supports the TCP) 7 applications (e.g., supports the SMTP) For systems including OSI protocols, layers 5 and 6 may also be counted."

SNMP-MPD-MIB

The MIB for Message Processing and Dispatching"

The following table lists the tables associated with this MIB:

MIB Name	Description
snmpUnknownPDUHandlers	" The total number of packets received by the SNMP engine which were dropped because the PDU contained in the packet could not be passed to an application responsible for handling the pduType, e.g. no SNMP application had registered for the proper combination of the contextEngineID and the pduType. "
snmpUnknownSecurityModels	" The total number of packets received by the SNMP engine which were dropped because they referenced a securityModel that was not known to or supported by the SNMP engine. "
snmpInvalidMsgs	" The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message. "

SNMP-NOTIFICATION-MIB

This MIB module defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of notifications.

The following table lists the tables associated with this MIB:

MIB Name	Description
snmpNotifyRowStatus	" The status of this conceptual row. To create a row in this table, a manager must set this object to either createAndGo(4) or createAndWait(5)."
snmpNotifyStorageType	" The storage type for this conceptual row."
snmpNotifyTag	" This object contains a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected."
snmpNotifyType	" This object determines the type of notification to be generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag. This value is only used when generating notifications, and is ignored when using the snmpTargetAddrTable for other purposes. If the value of this object is trap(1), then any messages generated for selected rows will contain Unconfirmed-Class PDUs. If the value of this object is inform(2), then any messages generated for selected rows will contain Confirmed-Class PDUs. Note that if an SNMP entity only supports generation of Unconfirmed-Class PDUs (and not Confirmed-Class PDUs), then this object may be read-only."

MIB Name	Description
snmpNotifyRowStatus	" The status of this conceptual row. To create a row in this table, a manager must set this object to either createAndGo(4) or createAndWait(5)."
snmpNotifyStorageType	" The storage type for this conceptual row."
snmpNotifyTag	" This object contains a single tag value which is used to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object contains a value of zero length, no entries are selected."

snmpNotifyType	" This object determines the type of notification to be generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag. This value is only used when generating notifications, and is ignored when using the snmpTargetAddrTable for other purposes. If the value of this object is trap(1), then any messages generated for selected rows will contain Unconfirmed-Class PDUs. If the value of this object is inform(2), then any messages generated for selected rows will contain Confirmed-Class PDUs. Note that if an SNMP entity only supports generation of Unconfirmed-Class PDUs (and not Confirmed-Class PDUs), then this object may be read-only."

SNMP-TARGET-MIB

This MIB module defines MIB objects which provide mechanisms to remotely configure the parameters used by an SNMP entity for the generation of SNMP messages."

The following table lists the tables associated with this MIB:

MIB Name	Description
snmpTargetAddrParams	" The value of this object identifies an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generating messages to be sent to this transport address."
snmpTargetAddrRetryCount	" This object specifies a default number of retries to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored."
snmpTargetAddrRowStatus	" The status of this conceptual row. To create a row in this table, a manager must set this object to either createAndGo(4) or createAndWait(5). Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the snmpTargetAddrRowStatus column is 'notReady'. In particular, a newly created row cannot be made active until the corresponding instances of snmpTargetAddrTDomain, snmpTargetAddrTAddress, and snmpTargetAddrParams have all been set. The following objects may not be modified while the value of this object is active(1): - snmpTargetAddrTDomain - snmpTargetAddrTAddress An attempt to set these objects while the value of snmpTargetAddrRowStatus is active(1) will result in an inconsistentValue error."
snmpTargetAddrStorageType	" The storage type for this conceptual row."

snmpTargetAddrTAddress	" This object contains a transport address. The format of this address depends on the value of the snmpTargetAddrTDomain object."
snmpTargetAddrTagList	" This object contains a list of tag values which are used to select target addresses for a particular operation."
snmpTargetAddrTDomain	" This object indicates the transport type of the address contained in the snmpTargetAddrTAddress object."
snmpTargetAddrTimeout	" This object should reflect the expected maximum round trip time for communicating with the transport address defined by this row. When a message is sent to this address, and a response (if one is expected) is not received within this time period, an implementation may assume that the response will not be delivered. Note that the time interval that an application waits for a response may actually be derived from the value of this object. The method for deriving the actual time interval is implementation dependent. One such method is to derive the expected round trip time based on a particular retransmission algorithm and on the number of timeouts which have occurred. The type of message may also be considered when deriving expected round trip times for retransmissions. For example, if a message is being sent with a securityLevel that indicates both authentication and privacy, the derived value may be increased to compensate for extra processing time spent during authentication and encryption processing."
snmpTargetParamsMPModel	" The Message Processing Model to be used when generating SNMP messages using this entry."
snmpTargetParamsRowStatus	" The status of this conceptual row. To create a row in this table, a manager must set this object to either createAndGo(4) or createAndWait(5). Until instances of all corresponding columns are appropriately configured, the value of the corresponding instance of the snmpTargetParamsRowStatus column is 'notReady'. In particular, a newly created row cannot be made active until the corresponding snmpTargetParamsMPModel, snmpTargetParamsSecurityModel, snmpTargetParamsSecurityName, and snmpTargetParamsSecurityLevel have all been set. The following objects may not be modified while the value of this object is active(1): - snmpTargetParamsMPModel - snmpTargetParamsSecurityModel - snmpTargetParamsSecurityName - snmpTargetParamsSecurityLevel An attempt to set these objects while the value of snmpTargetParamsRowStatus is active(1) will result in an inconsistentValue error."
snmpTargetParamsSecurityLevel	" The Level of Security to be used when generating SNMP messages using this entry."

snmpTargetParamsSecurityModel	" The Security Model to be used when generating SNMP messages using this entry. An implementation may choose to return an inconsistentValue error if an attempt is made to set this variable to a value for a security model which the implementation does not support."
snmpTargetParamsSecurityName	" The securityName which identifies the Principal on whose behalf SNMP messages will be generated using this entry."
snmpTargetParamsStorageType	" The storage type for this conceptual row."
snmpTargetSpinLock	" This object is used to facilitate modification of table entries in the SNMP-TARGET-MIB module by multiple managers. In particular, it is useful when modifying the value of the snmpTargetAddrTagList object. The procedure for modifying the snmpTargetAddrTagList object is as follows: 1. Retrieve the value of snmpTargetSpinLock and of snmpTargetAddrTagList. 2. Generate a new value for snmpTargetAddrTagList. 3. Set the value of snmpTargetSpinLock to the retrieved value, and the value of snmpTargetAddrTagList to the new value. If the set fails for the snmpTargetSpinLock object, go back to step 1."
snmpUnavailableContexts	" The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unavailable."
snmpUnknownContexts	" The total number of packets received by the SNMP engine which were dropped because the context contained in the message was unknown."

SNMP-FRAMEWORK-MIB

The SNMP Management Architecture MIB

The following table lists the tables associated with this MIB:

MIB Name	Description
snmpEngineBoots	" The number of times that the SNMP engine has (re-)initialized itself since snmpEngineID was last configured. "
snmpEngineID	" An SNMP engine's administratively-unique identifier. This information SHOULD be stored in non-volatile storage so that it remains constant across re-initializations of the SNMP engine. "
snmpEngineMaxMessageSize	" The maximum length in octets of an SNMP message which this SNMP engine can send or receive and process, determined as the minimum of the maximum message size values supported among all of the transports available to and supported by the engine. "

snmpEngineTime	" The number of seconds since the value of the snmpEngineBoots object last changed. When incrementing this object's value would cause it to exceed its maximum, snmpEngineBoots is incremented as if a re-initialization had occurred, and this object's value consequently reverts to zero. "

TCP-MIB

The MIB module for managing TCP implementations.

The following table lists the tables associated with this MIB:

MIB Name	Description
tcpActiveOpens	" The number of times that TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpAttemptFails	" The number of times that TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times that TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpConnectionProcess	" The system's process ID for the process associated with this connection, or zero if there is no such process. This value is expected to be the same as HOST-RESOURCES-MIB:: hrSWRunIndex or SYSAPPL-MIB::sysApplElmtRunIndex for some row in the appropriate tables."
tcpConnectionState	" The state of this TCP connection. The value listen(2) is included only for parallelism to the old tcpConnTable and should not be used. A connection in LISTEN state should be present in the tcpListenerTable. The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then the TCB (as defined in [RFC793]) of the corresponding connection on the managed node is deleted, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note, however, that RST segments are not sent reliably)."
tcpConnLocalAddress	" The local IP address for this TCP connection. In the case of a connection in the listen state willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used."

tcpConnLocalPort	" The local port number for this TCP connection."
tcpConnRemAddress	" The remote IP address for this TCP connection."
tcpConnRemPort	" The remote port number for this TCP connection."
tcpConnState	" The state of this TCP connection. The only value that may be set by a management station is deleteTCB(12). Accordingly, it is appropriate for an agent to return a `badValue' response if a management station attempts to set this object to any other value. If a management station sets this object to the value deleteTCB(12), then the TCB (as defined in [RFC793]) of the corresponding connection on the managed node is deleted, resulting in immediate termination of the connection. As an implementation-specific option, a RST segment may be sent from the managed node to the other TCP endpoint (note, however, that RST segments are not sent reliably)."
tcpCurrEstab	" The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT."
tcpEstabResets	" The number of times that TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpHCInSegs	" The total number of segments received, including those received in error. This count includes segments received on currently established connections. This object is the 64-bit equivalent of tcpInSegs. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpHCOutSegs	" The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. This object is the 64-bit equivalent of tcpOutSegs. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpInErrs	" The total number of segments received in error (e.g., bad TCP checksums). Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpInSegs	" The total number of segments received, including those received in error. This count includes segments received on currently established connections. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpListenerProcess	" The system's process ID for the process associated with this listener, or zero if there is no such process. This value is expected to be the same as HOST-RESOURCES-MIB:: hrSWRunIndex or SYSAPPL-MIB::sysApplElmtRunIndex for some row in the appropriate tables."

tcpMaxConn	" The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1."
tcpOutRsts	" The number of TCP segments sent containing the RST flag. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpOutSegs	" The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpPassiveOpens	" The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpRetransSegs	" The total number of segments retransmitted; that is, the number of TCP segments transmitted containing one or more previously transmitted octets. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime."
tcpRtoAlgorithm	" The algorithm used to determine the timeout value used for retransmitting unacknowledged octets."
tcpRtoMax	" The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend on the algorithm used to determine the retransmission timeout; in particular, the IETF standard algorithm rfc2988(5) provides an upper bound (as part of an adaptive backoff algorithm)."
tcpRtoMin	" The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend on the algorithm used to determine the retransmission timeout; in particular, the IETF standard algorithm rfc2988(5) provides a minimum value."

UDP-MIB

The MIB module for managing UDP implementations.Copyright (C) The Internet Society (2005). This version of this MIB module is part of RFC 4113; see the RFC itself for full legal notices."

The following table lists the tables associated with this MIB:

MIB Name	Description

udpEndpointProcess	" The system's process ID for the process associated with this endpoint, or zero if there is no such process. This value is expected to be the same as HOST-RESOURCES-MIB::hrSWRunIndex or SYSAPPL-MIB:: sysApplElmtRunIndex for some row in the appropriate tables."
udpHClnDatagrams	" The total number of UDP datagrams delivered to UDP users, for devices that can receive more than 1 million UDP datagrams per second. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."
udpHCOutDatagrams	" The total number of UDP datagrams sent from this entity, for devices that can transmit more than 1 million UDP datagrams per second. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."
udpInDatagrams	" The total number of UDP datagrams delivered to UDP users. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."
udpInErrors	" The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."
udpLocalAddress	" The local IP address for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used."
udpLocalPort	" The local port number for this UDP listener."
udpNoPorts	" The total number of received UDP datagrams for which there was no application at the destination port. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."
udpOutDatagrams	" The total number of UDP datagrams sent from this entity. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime."

MPLS-L3VPN-STD-MIB

This MIB contains managed object definitions for the Layer-3 Multiprotocol Label Switching Virtual Private Networks

The following table lists the tables associated with this MIB:

MIB Name	Description
mplsL3VpnActiveVrfs	" The number of VRFs that are active on this node. That is, those VRFs whose corresponding mplsL3VpnVrfOperStatus object value is equal to operational (1)."
mplsL3VpnConfiguredVrfs	" The number of VRFs that are configured on this node."
mplsL3VpnConnectedInterfaces	" Total number of interfaces connected to a VRF."
mplsL3VpnIllLblRcvThrsh	" The number of illegally received labels above which the mplsNumVrfSecIllglLblThrshExcd notification is issued. The persistence of this value mimics that of the device's configuration."
mplsL3VpnNotificationEnable	" If this object is true, then it enables the generation of all notifications defined in this MIB. This object's value should be preserved across agent reboots." REFERENCE " See also [RFC3413] for explanation that notifications are under the ultimate control of the MIB modules in this document."
mplsL3VpnVrfConfMaxPossRts	" Denotes maximum number of routes that the device will allow all VRFs jointly to hold. If this value is set to 0, this indicates that the device is unable to determine the absolute maximum. In this case, the configured maximum MAY not actually be allowed by the device."
mplsL3VpnVrfConfRteMxThrshTime	" Denotes the interval in seconds, at which the route max threshold notification may be reissued after the maximum value has been exceeded (or has been reached if mplsL3VpnVrfConfMaxRoutes and mplsL3VpnVrfConfHighRteThresh are equal) and the initial notification has been issued. This value is intended to prevent continuous generation of notifications by an agent in the event that routes are continually added to a VRF after it has reached its maximum value. If this value is set to 0, the agent should only issue a single notification at the time that the maximum threshold has been reached, and should not issue any more notifications until the value of routes has fallen below the configured threshold value. This is the recommended default behavior."

EVENT-MIB

The MIB module for defining event triggers and actions for network management purposes."

The following table lists the tables associated with this MIB:

MIB Name	Description

mteResourceSampleMinimum	" The minimum mteTriggerFrequency this system will accept. A system may use the larger values of this minimum to lessen the impact of constant sampling. For larger sampling intervals the system samples less often and suffers less overhead. This object provides a way to enforce such lower overhead for all triggers created after it is set. Unless explicitly resource limited, a system's value for this object SHOULD be 1, allowing as small as a 1 second interval for ongoing trigger sampling. Changing this value will not invalidate an existing setting of mteTriggerFrequency."
mteResourceSampleInstanceMaximum	" The maximum number of instance entries this system will support for sampling. These are the entries that maintain state, one for each instance of each sampled object as selected by mteTriggerValueID. Note that wildcarded objects result in multiple instances of this state. A value of 0 indicates no preset limit, that is, the limit is dynamic based on system operation and resources. Unless explicitly resource limited, a system's value for this object SHOULD be 0. Changing this value will not eliminate or inhibit existing sample state but could prevent allocation of additional state information."
mteResourceSampleInstances	" The number of currently active instance entries as defined for mteResourceSampleInstanceMaximum."
mteResourceSampleInstancesHigh	" The highest value of mteResourceSampleInstances that has occurred since initialization of the management system."
mteResourceSampleInstanceLacks	" The number of times this system could not take a new sample because that allocation would have exceeded the limit set by mteResourceSampleInstanceMaximum."
mteTriggerFailures	" The number of times an attempt to check for a trigger condition has failed. This counts individually for each attempt in a group of targets or each attempt for a wildcarded object."
mteEventFailures	" The number of times an attempt to invoke an event has failed. This counts individually for each attempt in a group of targets or each attempt for a wildcarded trigger object."
mteHotTrigger	" The name of the trigger causing the notification."
mteHotTargetName	" The SNMP Target MIB's snmpTargetAddrName related to the notification."
mteHotContextName	" The context name related to the notification. This MUST be as fully-qualified as possible, including filling in wildcard information determined in processing."
mteHotOID	" The object identifier of the destination object related to the notification. This MUST be as fully-qualified as possible, including filling in wildcard information determined in processing. For a trigger-related notification this is from mteTriggerValueID. For a set failure this is from mteEventSetObject."
mteHotValue	" The value of the object at mteTriggerValueID when a trigger fired."

mteFailedReason	" The reason for the failure of an attempt to check for a trigger condition or set an object in response to an event."

CISCO-IPSEC-FLOW-MONITOR-MIB.my

This is a MIB Module for monitoring the structures in IPSec-based Virtual Private Networks. The MIB has been designed to be adopted as an IETF standard. Hence Cisco-specific features of IPSec protocol are excluded from this MIB.
The following table lists the tables associated with this MIB:

MIB Name	Description
cipSecFailTableSize	" The window size of the IPsec Phase-1 and Phase-2 Failure Tables. The IPsec Phase-1 and Phase-2 Failure Tables are implemented as a sliding window in which only the last n entries are maintained. This object is used specify the number of entries which will be maintained in the IPsec Phase-1 and Phase-2 Failure Tables. An implementation may choose suitable minimum and maximum values for this element based on the local policy and available resources. If an SNMP SET request specifies a value outside this window for this element, a BAD VALUE may be returned."
cipSecTrapCntlIkeCertCrlFailure	" This object defines the administrative state of sending the IPsec IKE Phase-1 Certificate/CRL Failure TRAP"
cipSecTrapCntlIkeNoSa	" This object defines the administrative state of sending the IPsec IKE Phase-1 No Security Association TRAP"
cipSecTrapCntlIkeProtocolFail	" This object defines the administrative state of sending the IPsec IKE Phase-1 Protocol Failure TRAP"
cipSecTrapCntlIkeSysFailure	" This object defines the administrative state of sending the IPsec IKE Phase-1 System Failure TRAP"

cipSecTrapCntlIkeTunnelStart	" This object defines the administrative state of sending the IPsec IKE Phase-1 Tunnel Start TRAP"
cipSecTrapCntlIkeTunnelStop	" This object defines the administrative state of sending the IPsec IKE Phase-1 Tunnel Stop TRAP"
cipSecTrapCntlIpSecEarlyTunTerm	" This object defines the administrative state of sending the IPsec Phase-2 Early Tunnel Termination TRAP"
cipSecTrapCntlIpSecNoSa	" This object defines the administrative state of sending the IPsec Phase-2 No Security Association TRAP"
cipSecTrapCntlIpSecProtocolFail	" This object defines the administrative state of sending the IPsec Phase-2 Protocol Failure TRAP"
cipSecTrapCntlIpSecSetUpFailure	" This object defines the administrative state of sending the IPsec Phase-2 Set Up Failure TRAP"
cipSecTrapCntlIpSecSysFailure	" This object defines the administrative state of sending the IPsec Phase-2 System Failure TRAP"
cipSecTrapCntlIpSecTunnelStart	" This object defines the administrative state of sending the IPsec Phase-2 Tunnel Start TRAP"
cipSecTrapCntlIpSecTunnelStop	" This object defines the administrative state of sending the IPsec Phase-2 Tunnel Stop TRAP"

CISCO-BULK-FILE-MIB.my

The MIB module for creating and deleting bulk files of SNMP data for file transfer."
The following table lists the tables associated with this MIB:

MIB Name	Description
cbfDefineFiles	The maximum value of cbfDefineFiles since system initialization.
cbfDefineFilesRefused	The maximum value of cbfDefineObjects since system initialization.
cbfDefineHighFiles	The maximum number of file definitions this system can hold in cbfDefineFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number does not disturb existing entries.
cbfDefineHighObjects	The maximum total number of object selections to go with file definitions this system, that is, the total number of objects this system can hold in cbfDefineObjectTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number does not disturb existing entries.
cbfDefineMaxFiles	The current number of object selections in cbfDefineObjectTable.
cbfDefineMaxObjects	The number of attempts to create an object selection that failed due to exceeding cbfDefineMaxObjects.
cbfDefineObjects	The current number of file statuses in cbfStatusFileTable.
cbfDefineObjectsRefused	The number times the oldest entry was deleted due to exceeding cbfStatusMaxFiles.
cbfStatusFiles	The maximum value of cbfStatusFiles since system initialization.
cbfStatusFilesBumped	The maximum number of file statuses this system can hold in cbfStatusFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number deletes the oldest finished entries until the new limit is satisfied
cbfStatusHighFiles	The maximum value of cbfStatusFiles since system initialization
cbfStatusMaxFiles	" The maximum number of file statuses this system can hold in cbfStatusFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number deletes the oldest finished entries until the new limit is satisfied."
cbfStatusFiles	The maximum value of cbfStatusFiles since system initialization

cbfStatusFilesBumped	The number times the oldest entry was deleted due to exceeding cbfStatusMaxFiles.
cbfStatusHighFiles	The maximum value of cbfStatusFiles since system initialization
cbfStatusMaxFiles	The maximum number of file statuses this system can hold in cbfStatusFileTable. A value of 0 indicates no configured limit. This object may be read-only on some systems. Changing this number deletes the oldest finished entries until the new limit is satisfied

CISCO-AAA-SERVER-MIB.my

The MIB module for monitoring communications and status of AAA Server operation
The following table lists the tables associated with this MIB:

MIB Name	Description
casServerStateChangeEnable	" This variable controls the generation of casServerStateChange notification. When this variable is true(1), generation of casServerStateChange notifications is enabled. When this variable is false(2), generation of casServerStateChange notifications is disabled. The default value is false(2). "

CISCO-ENTITY-EXT-MIB

This MIB is an extension of the ENTITY-MIB specified in RFC2737.
The following table lists the tables associated with this MIB:

MIB Name	Description
ceExtEntBreakOutPortNotifEnable	" This object controls the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved as follows: 'true(1)' - the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved notifications is enabled. 'false(2)' - the generation of ceExtBreakOutPortInserted and ceExtBreakOutPortRemoved notifications is disabled."

ceExtEntDoorNotifEnable	" This object controls the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications as follows: 'true(1)' - the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications are enabled. 'false(2)' - the generation of ceExtEntDoorCloseNotif and ceExtEntDoorOpenNotif notifications are disabled."
CISCO-ENTITY-FRU-CONTROL-MIB.my	" The CISCO-ENTITY-FRU-CONTROL-MIB is used to monitor and configure operational status of Field Replaceable Units (FRUs) and other managable physical entities of the system listed in the Entity-MIB (RFC 2737) entPhysicalTable. FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc."
cefcFanTrayOperStatus	" The operational state of the fan or fan tray. unknown(1) - unknown. up(2) - powered on. down(3) - powered down. warning(4) - partial failure, needs replacement as soon as possible."
cefcFRUCurrent	" Current supplied by the FRU (positive values) or current required to operate the FRU (negative values)."
cefcFRUPowerAdminStatus	" Administratively desired FRU power state."
cefcFRUPowerOperStatus	" Operational FRU power state."
cefcMIBEnableStatusNotification	" This variable indicates whether the system produces the following notifications: cefcModuleStatusChange, cefcPowerStatusChange, cefcFRUInserted, cefcFRURemoved, cefcUnrecognizedFRU and cefcFanTrayStatusChange. A false value will prevent these notifications from being generated."
cefcModuleAdminStatus	" This object provides administrative control of the module."
cefcModuleLastClearConfigTime	" The value of sysUpTime when the configuration was most recently cleared."
cefcModuleOperStatus	" This object shows the module's operational state."

cefcModuleResetReason	" This object identifies the reason for the last reset performed on the module."
cefcModuleStatusLastChangeTime	" The value of sysUpTime at the time the cefcModuleOperStatus is changed."
cefcModuleUpTime	" This object provides the up time for the module since it was last re-initialized. This object is not persistent; if a module reset, restart, power off, the up time starts from zero."
cefcPhysicalStatus	" The status of this physical entity. other(1) - the status is not any of the listed below. supported(2) - this entity is supported. unsupported(3) - this entity is unsupported. incompatible(4) - this entity is incompatible. It would be unsupported(3), if the ID read from Serial EPROM is not supported. It would be incompatible(4), if in the present configuration this FRU is not supported."

IEEE8023-LAG-MIB

The IEEE8023-LAG-MIB is the Link Aggregation module for managing IEEE Std. 802.3ad.

Table 3-157 lists the tables associated with this MIB.

Table 3-157 IEEE8023-LAG-MIB Tables and Descriptions

Name	Description
dot3adAggTable	Table that contains information about every Aggregator running the IEEE 802.3ad Link Aggregation Control Protocol that is associated with this System

CISCO-P2P-IF-MIB

Table 3-157 IEEE8023-LAG-MIB Tables and Descriptions (continued)

Name	Description
dot3adAggPortListTable	Table that contains a list of all the ports associated with each Aggregator running the IEEE 802.3ad Link Aggregation Control Protocol.
dot3adAggPortTable	Table that contains Link Aggregation Control configuration information about every Aggregation Port running the IEEE 802.3ad Link Aggregation Control Protocol associated with this device. A row appears in this table for each physical port
dot3adAggPortStatsTable	Table that contains Link Aggregation information about every port running the IEEE 802.3ad Link Aggregation Control Protocol that is associated with this device. A row appears in this table for each physical port
dot3adAggPortDebugTable	Table that contains Link Aggregation debug information about every port running the IEEE 802.3ad Link Aggregation Control Protocol that is associated with this device. A row appears in this table for each physical port

dot3adTablesLastChanged	This object indicates the time of the most recent change to the dot3adAggTable, dot3adAggPortListTable or dot3AggPortTable.

MIB Constraints

Table 3-158 lists the constraints on objects in the IEEE8023-LAG-MIB.

Table 3-158 IEEE8023-LAG-MIB Constraints

MIB Object	Notes
dot3adAggPortListTable	dot3adAggPortListPorts is not supported.
dot3adAggActorSystemPriority	Not supported
dot3adAggActorAdminKey	Not supported
dot3adAggCollectorMaxDelay	Not supported
dot3adAggPortActorSystemPriority	Not supported
dot3adAggPortActorAdminKey	Not supported
dot3adAggPortActorOperKey	Not supported
dot3adAggPortPartnerAdminSystemPriority	Not supported
dot3adAggPortPartnerAdminSystemID	Not supported
dot3adAggPortPartnerAdminKey	Not supported

dot3adAggPortActorPortPriority	Not supported
dot3adAggPortPartnerAdminPort	Not supported
dot3adAggPortPartnerAdminPortPriority	Not supported

IEEE8021-CFM-MIB

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

Table 3-159 lists the tables associated with this MIB.

Name	Descriptions
dot1agCfmStackTable	This MIB table lists the Maintenance Points (MPs) that exist on each interface.
dot1agCfmVlanTable	This MIB table lists the VLAN IDs associated with each service (Maintenance Association or MA). In IOS-XR, services are not associated with VLAN IDs (rather they are associated with Bridge Domains), hence this table is unsupported.
dot1agCfmDefaultMdTable	The default Maintenance Domain (MD) level table is unsupported, since the concept of a default MD level does not exist in the IOS-XR implementation of CFM.

dot1agCfmConfigErrorListTable	This table exports four configuration errors described in the 802.1ag standard. Of the four errors, two cannot be detected due to the distributed nature of the IOS-XR implementation (CFMleak and ConflictingVids), and two never occur (ExcessiveLevels and OverlappedLevels). Therefore, an empty table is returned.
dot1agCfmMdTable	This MIB table lists the MDs that are configured.
dot1agCfmMaNetTable	This MIB table lists the MAs that are configured for each MD.
dot1agCfmMaCompTable	This MIB table lists the MAs that are configured for each MD, within each 'bridge component' in the router. This is to

MIB Constraints

Table 3-160 lists the constraints on objects in the IEEE8021-CFM-MIB.

Table 3-156 IEEE8021-CFM-MIB Constraints

MIB Object		Notes
dot1agCfmMdMaNextIndex		Always 0
dot1agCfmMdMhfCreation		Not supported
dot1agCfmMdMhfIdPermission		Always sendIdChassis(2)
dot1agCfmMdRowStatus		Always 'active'
dot1agCfmMaNetRowStatus		Always 'active'

dot1agCfmMaComponentId	Always '1'
dot1agCfmMaCompPrimaryVlanId	Not supported
dot1agCfmMaCompIdPermission	Always sendIdChassis(2)
dot1agCfmMaCompNumberOfVids	Not supported
dot1agCfmMaCompRowStatus	Always 'active'
dot1agCfmMaMepListRowStatus	Always 'active'
dot1agCfmMepActive	Not supported
dot1agCfmMepErrorCcmLastFailure	Not supported
dot1agCfmMepFngAlarmTime	Always 2.5s
dot1agCfmMepFngResetTime	Always 10s
dot1agCfmMepLowPrDef	Supported, if there is no 'Report Defects' configuration, or the 'Report Defects' configuration is compatible with the IEEE defects sets. Unsupported otherwise.
dot1agCfmMepPrimaryVid	Not supported
dot1agCfmMepRowStatus	Always 'active'
dot1agCfmMepTransmitLbmDataTlv	Not supported
dot1agCfmMepTransmitLbmDestIsMepId	Not supported
dot1agCfmMepTransmitLbmDestMacAddress	Not supported
dot1agCfmMepTransmitLbmDestMepId	Not supported
dot1agCfmMepTransmitLbmMessages	Not supported
dot1agCfmMepTransmitLbmResultOK	Not supported
dot1agCfmMepTransmitLbmSeqNumber	Not supported
dot1agCfmMepTransmitLbmStatus	Not supported
dot1agCfmMepTransmitLbmVlanDropEnable	Not supported

dot1agCfmMepTransmitLbmVlanPriority	Not supported
dot1agCfmMepTransmitLtmEgressIdentifier	Not supported
dot1agCfmMepTransmitLtmFlags	Not supported
dot1agCfmMepTransmitLtmResult	Not supported
dot1agCfmMepTransmitLtmSeqNumber	Not supported
dot1agCfmMepTransmitLtmStatus	Not supported
dot1agCfmMepTransmitLtmTargetIsMepId	Not supported
dot1agCfmMepTransmitLtmTargetMacAddress	Not supported
dot1agCfmMepTransmitLtmTargetMepId	Not supported
dot1agCfmMepTransmitLtmTtl	Not supported
dot1agCfmMepXconCcmLastFailure	Not Supported
dot1agCfmLtrReceiveOrder	Supported; the entries are not returned in the actual order they were received.

Chapter 4 - Monitoring Notifications

This chapter describes the Cisco NCS 4000 Series router notifications supported by the MIB enhancements feature introduced in Cisco IOS XR Software Release 3.7. SNMP uses notifications to report events on a managed device. The notifications are traps for different events. The router also supports other notifications not listed.

This chapter contains the following sections:

SNMP Notification Overview

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

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

When an agent detects an alarm condition, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host SNMP notifications are sent as one of the following:
- Traps—Unreliable messages, which do not require receipt acknowledgement from the SNMP manager.

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

Many commands use the keyword **traps** in the command syntax.

Note: Most notification types are disabled by default. However, some notification types cannot be controlled with the **snmp** command. For example, some notification types can be enabled by **snmp** or CLI and other types are enabled by a combination of CLI and **snmp**. The linkUpDown notifications are controlled by the **snmp trap link-status** and **snmp-server trap link ietf** commands.

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

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. The enabling command also specifies which types of traps are enabled.

- 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 the following URL:
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37snmp.html

Note: If you issue the **snmp-server 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:

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

Note: In the following tables, where *"no action is required"* is documented, there might be instances where an application, such as trouble ticketing, occurs. For detailed information, go to the following URL:
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/system_management/command/reference/yr37snmp.htmlManaging Physical Entities
This section describes how to use SNMP to manage the physical entities (components) in the router by:

- Performing Inventory Management, page 243

Purpose and Benefits

The physical entity management feature of the Cisco NCS 4000 Series router SNMP implementation does the following:

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

MIBs Used for Physical Entity Management

- CISCO-ENTITY-ASSET-MIB—Contains asset tracking information (IDPROM contents) for the physical entities listed in the entPhysicalTable of the ENTITY-MIB. The MIB provides device-specific information for physical entities, including orderable part number, serial number, manufacturing assembly number, and hardware, software, and firmware information.
- CISCO-ENTITY-FRU-CONTROL-MIB—Contains objects used to monitor and configure the administrative and operational status of field-replaceable units (FRUs), such as fans, RSPs, and transceivers that are listed in the entPhysicalTable of the ENTITY-MIB.
- CISCO-ENTITY-SENSOR-MIB—Contains information about entities in the entPhysicalTable with an entPhysicalClass value of sensor.
- ENTITY-MIB—Contains information for managing physical entities on the router. It also organizes the entities into a containment tree that depicts their hierarchy and relationship to each other.
- The MIB contains the following tables:
  - The entPhysicalTable describes each physical component (entity) in the router. The table contains an entry for the top-level entity (the chassis) and for each entity in the chassis. Each entry provides information about that entity: its name, type, vendor, and a description, and a description of how the entity fits into the hierarchy of chassis entities.
    Each entity is identified by a unique index (entPhysicalIndex) that is used to access information about the entity in this and other MIBs.
  - The entAliasMappingTable maps each physical port's entPhysicalIndex value to its corresponding ifIndex value in the IF-MIB ifTable.
  - The entPhysicalContainsTable shows the relationship between physical entities in the chassis. For each physical entity, the table lists the entPhysicalIndex for each of the entity's child objects.

Performing Inventory Management

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

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

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

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

Sample of ENTITY-MIB entPhysicalTable Entries

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

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

The following display shows the ENTITY-MIB entPhysicalTable sample entries:

```
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16288 = STRING: " CCC-RP0 Control Ethernet Port 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16289 = STRING: " CCC-RP1 Control Ethernet Port 1"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16291 = STRING: " ZYNQ (Erebor) Control Ethernet Port 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16292 = STRING: " DIGI G4 #0 Management Port"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16293 = STRING: " DIGI G4 #1 Management Port"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16294 = STRING: " ZYNQ - Control Ethernet Port 1"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16295 = STRING: " RP0 - Control Ethernet Port 24"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16296 = STRING: " RP1 - Control Ethernet Port 25"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16297 = STRING: " Jericho - Control Ethernet Port 26"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16298 = STRING: " Daughter card"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16385 = STRING: " NCS 4000 400G Packet/OTN/WDM - QSFP28/CFP2
- Line Card"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16386 = STRING: " CCC FPGA Thorin Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16387 = STRING: " CCC PON FPD Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16388 = STRING: " PCI Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16390 = STRING: " Ethernet Switch Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16391 = STRING: " NCS 4000 400G Packet/OTN/WDM - QSFP28/CFP2
- Line Card"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16392 = STRING: " Scratch IDPROM Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16404 = STRING: " I2C Module - Bus0"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16407 = STRING: " I2C Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.16408 = STRING: " I2C Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.39503 = STRING: " Board Voltage Sensor"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.39504 = STRING: " Board Current Sensor"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.39505 = STRING: " Voltage Sensor"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40864 = STRING: " Ethernet Switch Module"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40865 = STRING: " CCC-RP0 Control Ethernet Port 0"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40866 = STRING: " CCC-RP1 Control Ethernet Port 4"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40867 = STRING: " ZYNQ-DOP Control Ethernet Port 8"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40868 = STRING: " DIGI 0 Ethernet Port 12"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40869 = STRING: " DIGI1 - Control Ethernet Port 16"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40870 = STRING: " ZYNQ-ARM Control Ethernet Port 20"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40871 = STRING: " RP0 - Control Ethernet Port 24"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40872 = STRING: " RP1 - Control Ethernet Port 25"
SNMPv2-SMI::mib-2.47.1.1.1.1.2.40873 = STRING: " ARADPLUS - Control Ethernet Port 26"
```

Glossary

B

bandwidth	The difference between the highest and lowest frequencies available for network signals. The term is also used to describe the rated throughput capacity of a given network medium or protocol.
broadcast storm	Undesirable network event in which many broadcasts are sent simultaneously across all network segments. A broadcast storm uses substantial network bandwidth and, typically, causes network time-outs

C

CANA	Cisco Assigned Numbers Authority. The central clearing house for allocation of unique names and numbers that are embedded in Cisco software.
CLI	command-line interface
CNEM	Consistent Network Element Manageability
columnar object	One type of managed object that defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects (for example, ifTable in the IF-MIB defines the interface).
community name	Defines an access environment for a group of NMSs. NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.
critical alarm severity type	Indicates a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week. For example, online insertion and removal of line cards or loss of signal failure when a physical port link is down.
CWDM	Coarse Wavelength Division Multiplexing

D

dBm	Decibel (milliwatts). 10 * log10 (power in milliwatts). For example, 2 milliwatts is 10 * log10 (2) = 10 * 0.3010 = 3.01 dBm
DF	Delay Factor. The maximum observed value of the flow rate imbalance over a measurement interval.
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.

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.
Expected Packets	This value is formally defined as the extended last sequence number received less the initial sequence number received. An extended last sequence number is a 32-bit value, where the most significant 16-bit word indicates the number of sequence number cycles, and the least significant 16-bit word indicates the highest sequence number received.
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, and the blower fans.
Flow Metric	A measurement that reflects the quality of a traffic flow.
Flow Monitor	A hardware or software entity that classifies traffic flows, collects flow data, and periodically computes flow metrics
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.
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.
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 the 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.
IETF	The Internet Engineering Task Force
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 that holds the interface description (from MIB-II) ifDescr.
info	Notification about a condition that could lead to an impending problem or notification of an event that improves operation.
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 RFC 1213 and RFC 2233. Interfaces can have several layers, depending on the media, and each sublayer is represented by a separate row in the table. The relationship between the higher layer and lower layers is described in the ifStackTable.
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.
Inter-Arrival Jitter	An estimate of the statistical variance of the RTP data packet inter-arrival time. The inter-arrival jitter, J, is formally defined to be the mean deviation (smoothed absolute value) of the difference, D, in packet spacing at the flow monitor compared to the sender for a pair of packets. This is equivalent to the difference in the relative transit time for two packets; the relative transit time is the difference between a packet's RTP timestamp and the device's clock at the time of arrival (measured in the same units): D(i,j) = (Rj - Ri) - (Sj - Si) = (Rj - Sj) - (Ri - Si) where Si is the RTP timestamp from packet i, and Ri is the time of arrival in RTP timestamp units for packet i. The inter-arrival jitter SHOULD be calculated continuously for each RTP data packet received from source SSRCn, using this equation to compute difference for each packet and the previous packet (in order of arrival, not necessarily in sequence). |D(i-1,i)| - J(i-1) J(i) = J(i-1) + ---------- 16
IP Address	The variable hostConfigAddr indicates the IP address of the host that provided the host configuration file for a device.
K	
keepalive message	Message sent by one network device to inform another network device that the virtual circuit between the two is still active.
L	

label	A short, fixed-length identifier that is used to determine the forwarding of a packet.
LDP	Label Distribution Protocol
Loss Distance	The difference between the sequence numbers delimiting the start of two consecutive loss intervals. Consider the following sequence of RTP data packets: 111111 111222 2233 33333 444 444 5 123456x890123xxxx8901xxx56789x123xx678x0 ^ ^ ^ ^ ^ ^ | | | | | LI1 LI2 LI3 LI4 LI5 LI6 Loss Interval | Loss Distance ==========+========== 1 | 2 | 7 3 | 8 4 | 8 5 | 4 6 | 5
Loss Fraction	The fraction of RTP data packets from source SSRCn lost during a measurement interval, expressed as a fixed-point number: Li Fi = ---- Ei where Fi is the loss fraction for measurement interval i, Li is the lost packets during measurement interval i, and Ei is the expected packets during measurement interval i. Observe that the number of packets lost includes packets that are late or duplicates, and hence this number can can have a theoretical theoretical value between negative infinity and one. The cumulative loss fraction is the fraction of RTP data packets from source SSRCn lost over the duration monitoring the flow: n sum [Li] i=1 Fn = ---------- n sum [Ei] i=1 where Fn is the cumulative loss fraction over n measurement intervals.
Loss Interval	An interval in which consecutive packet losses were experienced. Consider the following sequence of RTP data packets: 111111 111222 2233 33333 444 444 5 123456x890123xxxx8901xxx56789x123xx678x0 ^ ^ ^ ^ ^ ^ | | | | | LI1 LI2 LI3 LI4 LI5 LI6 LI1 through LI6 indicates the start of loss intervals observed in this sequence.
Loss Interval Duration	The number of packets lost in a loss interval. Consider the following sequence of RTP data packets: 111111 111222 2233 33333 444 444 5 123456x890123xxxx8901xxx56789x123xx678x0 ^ ^ ^ ^ ^ ^ | | | | | LI1 LI2 LI3 LI4 LI5 LI6 Loss Interval | Duration ==========+========== 1 | 1 2 | 4 3 | 3 4 | 1 5 | 2 6 | 1
Lost Packets	This value is formally defined as the number of packets expected less the number of packets actually received, where the number of packets received includes those which are late or duplicates
LR	Long Reach
LSR	Label Switching Router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.
LSP	Label Switched Path
LX/LH	Long wavelength/long haul
M	
major alarm severity type	Used for hardware or software conditions. Indicates a serious disruption of service or the malfunctioning or failure of important hardware. Requires immediate attention and response of a technician to restore or maintain system stability. The urgency is less than in critical situations because of a lesser effect on service or system performance.
Measurement Interval	The length of time over which a flow monitor collects data related to a traffic flow, after which the flow monitor computes flow metrics using the collected data
Media Loss Rate	The number of lost or out-of-order packets over a measurement interval
Media Rate	The effective bit rate of the media content carried by a traffic flow.

minor alarm severity type	Used for troubles that do not have a serious effect on service to customers or for alarms in hardware those 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.
MLR	Media Loss Rate
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).
MR	Media Rate
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, Public Switched Telephone Network (PSTN).
NHLFE	Next Hop Label Forwarding Entry
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.
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

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.

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.

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 A read-only 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 A read-write variable can be used to monitor information and to set a new value for the variable. For example, the tsMsgSend variable, whose access is read-write, determines what action to take after a message has been sent.
The possible integer values for this variable follow:
1 = nothing
2 = reload
3 = message done
4 = abort

RFC Requests for Comments, started in 1969, form a series of notes about the Internet (originally the ARPANET). The notes discuss many aspects of computer communication, focusing on networking protocols, procedures, programs, and concepts, but also include meeting notes, opinions, and sometimes humor.

The 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.

RSVP Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so forth) of the packet streams they want to receive. RSVP depends on IPv4. Also known as Resource Reservation Setup Protocol.

S

scalar object One type of managed object that is a single object instance (for example, ifNumber in the IF-MIB and bgpVersion in the BGP4-MIB).

security model A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

SEEPROM Serial Electrically Erasable Programmable Read-only Memory

SR Short Reach

SNMPv1 The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings. SNMPv1 uses a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address access control list and password.

SNMPv2 The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.

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

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

SNMPv3 SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:

- Message integrity—Ensuring that a packet has not been tampered with in transit.
- Authentication—Determining that the message is from a valid source.
- Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMP agent A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent.

SNMP manager	A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces.
SSRCn	The SSRC identifier of the source.
SX	Short wavelength
T	
TE	Traffic engineered
time stamp	Provides the amount of time that has elapsed between the last network re-initialization and generation of the trap.
TLV	Type Length Value. Dynamic format for storing data in any order. Used by the Cisco 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.
Traffic Flow	A unidirectional stream of packets conforming to a classifier. For example, packets having a particular source IP address, destination IP address, protocol type, source port number, and destination port number.
Transit Time	The latency from the insertion into the network to the flow monitor. This value can be computed by taking the difference between a packet's RTP timestamp and the device's clock at the time of arrival (measured in the same units).
trap	An trap is an unsolicited (device-initiated) message. The contents of the message might be simply informational, but it is mostly used to report real-time trap information. Because a trap is a UDP datagram, sole reliance upon them to inform you of network problems (for example, passive network monitoring) is not wise. A trap can be used in conjunction with other SNMP mechanisms, as in trap-directed polling,
tunnel	A secure communication path between two peers, such as routers.
U	
UDI	Cisco Unique Device Identifier
UDP	User Datagram Protocol
V	
VRF	VPN Routing and Forwarding Tables
VB	Virtual Buffer. A virtual buffer is a construct used to simulate a real buffer used by a media application for the purpose of storing media packets until the application can render their content.
VTP	VLAN Trunking Protocol
W	
WFQ	Weighted Fair Queueing

write-only	The write-only 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	
XCVR	Transceiver