Cisco MDS 9000 Family MIB Quick Reference

Text Part Number: OL-29317-01
April, 2014

The *Cisco MDS 9000 Family MIB Quick Reference Reference* describes the Management Information Base (MIB) files for the Cisco MDS 9000 Family of multilayer directors and fabric switches. The Cisco MIB files are provided with all Cisco MDS NX-OS and SAN-OS software releases. The MIB files contain variables that can be set or read to provide information about network devices and interfaces.

This document provides the following information:

MIBs and Network Management

This document lists MIBs as well as many other Internet Engineering Task Force (IETF) standard MIBs. These MIBs are defined in documents called *Requests for Comments* (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco MDS 9000 Family.

From the perspective of a network manager, network management takes place between two major types of systems: those in control, called *managing systems*, and those observed and controlled, called *managed systems*. The most common managing system is called a *network management system* (NMS). Managed systems can include hosts, servers, or network components such as switches or intelligent repeaters. CiscoWorks is an example of an NMS.

To promote interoperability, cooperating systems must adhere to a common framework and a common language, called a *protocol*. In the Internet-standard management framework, that protocol is the Simple Network Management Protocol (SNMP).

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The exchange of information between managed network devices and a robust NMS is essential for reliable performance of a managed network. Because some devices have a limited ability to run management software, most of the computer processing burden is assumed by the NMS. The NMS runs the network management applications, such as Fabric Manager, that present management information to network managers and other users.

In a managed device, specialized low-impact software modules, called *agents*, access information about the device and make it available to the NMS. Managed devices maintain values for a number of variables and report those, as required, to the NMS. For example, an agent might report such data as the number of bytes and packets sent or received by the device or the number of broadcast messages sent and received. In SNMP, each of these variables is referred to as a *managed object*. A managed object is anything that can be managed, anything that an agent can access and report back to the NMS. All managed objects are contained in the MIB, which is a database of the managed objects.

An NMS can control a managed device by sending a request to an agent of that managed device, requiring the device to change the value of one or more of its variables. The managed devices can respond to requests such as **set** or **get**. The NMS uses the **set** request to control the device. The NMS uses the **get** requests to monitor the device. The **set** and **get** requests are synchronous events, meaning the NMS initiates the activity, and the SNMP agent responds.

The managed device can send asynchronous events, or SNMP notifications, to the NMS to inform the NMS of some recent event. SNMP notifications (traps or informs) are included in many MIBs and help to alleviate the need for the NMS to frequently send get requests to the managed devices.

Accessing MIB Variables Through SNMP

You can access the Cisco MIB variables through SNMP. The SNMP system consists of three parts: SNMP manager, SNMP agent, and MIB. You can compile Cisco MIBs with your network management software. If SNMP is configured on a device, the SNMP agent responds to MIB-related queries sent by the NMS.

Table 1 describes the SNMP operations.

Table 1 SNMP Operations

Operation	Description
get-request	Retrieves a value from a specific variable.
get-next-request	Retrieves the value following the named variable. Often used to retrieve variables from within a table.[1]
get-bulk[2]	Retrieves large blocks of data, such as multiple rows in a table, which would otherwise require the transmission of many small blocks of data.
set-request	Stores a value in a specific variable.
response	Replies to the above commands sent by an NMS and to the informs sent by an agent.
trap	Sends an unsolicited message by an SNMP agent to an SNMP manager indicating that some event has occurred.
inform[2]	Sends an unsolicited message by an SNMP agent to an SNMP manager indicating that some event has occurred. Differs from a trap in that an acknowledgement is required from the manager.

1.With this operation, an SNMP manager does not need to know the exact variable name. A sequential search finds the next variable from within the MIB.
2.The **get-bulk** and **inform** commands are not a part of SNMPv1.

SNMP has been updated twice since its inception. SNMPv1 is the initial version of the protocol. SNMPv2 added support for 64-bit counters, and SNMPv3 added robust security for access, authentication, and encryption of managed data.

SNMP Traps and Informs

You can configure the Cisco MDS 9000 Family switch to send notifications to SNMP managers when particular events occur. You can send these notifications as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

Notifications may contain a list of MIB variables or varbinds that clarify the status being relayed by the notification. The list of varbinds associated with a notification is included in the notification definition in the MIB. In the case of standard MIBs, Cisco has enhanced some notifications with additional varbinds that further clarify the cause of the notification. See the "Extending the IF-MIB" section on page 42 for an example of this in the IF-MIB.

Use the SNMP-TARGET-MIB to obtain more information on trap destinations and inform requests.

Note Notifications must be enabled through SNMP, Fabric Manager, or the CLI.

Interpreting the MIB Structure

A MIB presents the managed data in a logical tree hierarchy, using an IETF standard syntax called the Structure of Management Information (SMI). Branches of this MIB tree are organized into individual tables, which contain the managed data as leaf objects. Understanding these concepts is fundamental to interpreting the management information provided by the MIB.

This section provides the following information:

Object Identifiers

The MIB structure is logically represented by a tree hierarchy. The *root* of the tree is unnamed and splits into three main branches: Consultative Committee for International Telegraph and Telephone (CCITT), International Organization for Standardization (ISO), and joint ISO/CCITT.

These branches and those that fall below each category have short text strings and integers to identify them. Text strings describe *object names*, while integers allow computer software to create compact, encoded representations of the names.

Each MIB variable is assigned an object identifier. The *object identifier* is the sequence of numeric labels on the nodes along a path from the root to the object. For example, the MIB variable tftpHost is indicated by the number 1. The object identifier for tftpHost is iso.org.dod.internet.private.enterprise.cisco.workgroup products.stack group.tftp group.tftpHost or *.1.3.6.1.4.1.9.5.1.5.1*. The last value is the number of the MIB variable tftpHost.

Tables

When network management protocols use names of MIB objects in messages, each name has an appended suffix. This suffix is called an *instance identifier*. It identifies one occurrence of the associated MIB object. For simple scalar objects, the instance identifier 0 refers to the instance of the object with that name (for example, sysUpTime.0).

A MIB also can contain tables of related objects. For example, ifOperStatus is a MIB object inside the ifTable from the IF-MIB. It reports the operational state for an interface on a device. Because devices may have more than one interface, it is necessary to have more than one instance of ifOperStatus. This instance value is added to the end of the MIB object as the instance identifier (for example, ifOperStatus.2 reports the operational state for interface number 2).

Each object in a table is constructed with a set of clauses defined by the SMI. These clauses include the SYNTAX clause, MAX-ACCESS clause, STATUS clause, and DESCRIPTION clause.

An excerpt of the information in the VSAN table (known as vsanTable) from CISCO-VSAN-MIB follows:

```
vsanTable OBJECT-TYPE
        SYNTAX     SEQUENCE OF VsanEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
        "A table of VSANs configured on this device."
       ::= { vsanConfiguration 3 }
vsanEntry OBJECT-TYPE
        SYNTAX     VsanEntry
        MAX-ACCESS not-accessible
        STATUS     current
        DESCRIPTION
               "An entry (conceptual row) in the vsanTable."
        INDEX { vsanIndex }
        ::= { vsanTable 1 }
VsanEntry ::= SEQUENCE {
        vsanIndex                 VsanIndex,
        vsanName                  SnmpAdminString,
       }
```

In the example, vsanTable contains two variables: vsanIndex and vsanName. (There are more values in the actual vsanTable.) The index for this table is the ID of the VSAN, or vsanIndex. With *n* number of VSANs configured, *n* rows are present in the table. If you want to retrieve the vsanName that matches VSAN ID 3 (vsanIndex is 3), then you would issue an SNMP **get** for vsanName.3.

SYNTAX Clause

The SYNTAX clause describes the format of the information, or value, that is returned when you monitor or set information in a MIB.

The Cisco MDS 9000 Family MIBs are defined with the SNMPv2 Structure of Management Information version 2 (SNMPv2-SMI) defined in RFC 1902. Some examples of SNMPv2-SMI syntax are as follows:

- Counter32—A nonnegative integer that increases until it reaches some maximum value. After reaching the maximum value, it rolls over to zero. For example, the variable ifInOctets, with a Counter32 syntax, counts the number of input octets on an interface.
- Gauge32—A nonnegative integer that increases until it reaches some maximum value. After reaching the maximum value, it stays fixed (no roll over).
- Counter64—A nonnegative 64-bit integer that increases until it reaches some maximum value. After reaching the maximum value, it rolls back to zero. Counter64 is used for MIB objects that can reach high values in a short period of time (for example, a packet counter for a Gigabit Ethernet port).
- Integer32—An integer from -2^{32} to $2^{32}-1$.
- IPAddress—An octet string that represents an IP address. For example, the variable hostConfigAddr indicates the IP address of the host that provided the host configuration file for a device.
- Timeticks—A nonnegative integer that counts the hundredths of a second that have elapsed since an event. For example, the variable loctcpConnElapsed provides the length of time that a TCP connection has been established.

MAX-ACCESS Clause

The MAX-ACCESS clause identifies the maximum access level for the associated MIB object. This clause can represent one of the following five states: read-create, read-write, read-only, accessible-for-notify, and not-accessible.

- read-create—You can read, modify, or create objects as rows in a table.
- read-write—You can read or modify this object.
- read-only—You can only read this object.
- accessible-for-notify—You cannot read or write to this object. SNMP notifications can send this object as part of their event information.
- not-accessible—You cannot read or write to this object. Table indices are typically objects that are not accessible.

AGENT-CAPABILITIES

In SNMP, capabilities files provide implementation details for the associated MIB. These files, called AGENT-CAPABILITIES, list supported conformance groups and any deviations from the MIB as implemented in the associated software version. For instance, the CISCO-AAA-SERVER-CAPABILITY provides the implementation details for the CISCO-AAA-SERVER-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

Note Capabilities files may have implementation details for more than one software release. You need to match your software release to the corresponding AGENT-CAPABILITIES clause in this file.

About Cisco MIB Files

The Cisco MDS 9000 Family MIB files can be obtained by File Transfer Protocol (FTP) from http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml, under Cisco Storage Networking.

Cisco MIB files are a set of objects that are private extensions to the IETF standard MIB II. MIB II is documented in RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*. Portions of MIB-II have been updated since RFC 1213. See the IETF website http://www.ietf.org for the latest updates to this MIB.

If your NMS cannot get requested information from a managed device, such as a Cisco switch, the MIB that allows that specific data collection might be missing. Typically, if an NMS cannot retrieve a particular MIB variable, either the NMS does not recognize the MIB variable, or the agent does not support the MIB variable. If the NMS does not recognize a specified MIB variable, you might need to load the MIB into the NMS, usually with a MIB compiler. For example, you might need to load the Cisco private MIB or the supported RFC MIB into the NMS to execute a specified data collection. If the agent does not support a specified MIB variable, you must find out what version of system software you are running. Different software releases support different MIBs.

Note Cisco and IETF MIBs are updated frequently. You should download the latest MIBs from http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml whenever you upgrade your Cisco MDS NX-OS or SAN-OS.

Cisco MIB File Directories

Cisco MIB files are organized into two directories: SNMPv1-SMI MIBs are in the SNMPv1 directory, and SNMPv2-SMI MIBs are in the SNMPv2 directory. The list of supported MIBs for the Cisco MDS 9000 Family is available at

ftp://ftp.cisco.com/pub/mibs/supportlists/mds9000/MDS9000MIBSupportList.html

Cisco also includes supported IETF-standard MIBs at this website. Use this support list to access and download the individual MIB files.

MIB Loading Order

Many MIBs use definitions that are defined in other MIBs. These definitions are listed in the IMPORTS section near the top of the MIB.

For example, if MIB B imports a definition from MIB A, some MIB compilers require you to load MIB A prior to loading MIB B. If you get the MIB loading order wrong, you might get an error message about what was imported, claiming it is undefined or not listed in IMPORTS. If you receive an error, look at the loading order of the MIB definitions from the IMPORTS of the MIB. Make sure that you have loaded all the preceding MIBs first.

Here is a list of MIBs from which many other MIBs import definitions. The MIBs are listed in the order in which you should load them:

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

- CISCO-ST-TC.my
- CISCO-VSAN-MIB.my
- ENTITY-MIB.my

If you load the MIBs in this order, you can eliminate most of your load-order definition problems. You can load most other MIBs (those not listed here) in any order.

Accessing and Downloading Cisco MIB Files

You can access the Cisco MIB files in either of the following ways:

- Using HTTP to Access and Download the MIB Files from CCO, page 7
- Using Passive FTP to Access and Download the MIB Files, page 8

Note You can also access and download Cisco MIB files using the SNMP Object Navigator tool located at the following site: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en. You can use this tool to translate SNMP object identifiers (OIDs) into object names, search object names, and descriptions, browse OID trees, and download MIB files.

Using HTTP to Access and Download the MIB Files from CCO

To access MIB files using your Web browser, follow these steps:

Step 1 Enter the following URL in the Address field:

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

Step 2 Select **Cisco Storage Networking**.

Step 3 Select **Cisco MDS 9000 Family**.

Step 4 Select and save each MIB you need to download from the Cisco MDS 9000 Family MIB support list.

If you are using Internet Explorer, you might need to enable passive FTP. To enable passive FTP, follow these steps:

Step 1 Open Internet Explorer, and click **Tools > Internet Options**.

Step 2 Click the **Advanced** tab on the top of the window.

Step 3 Scroll down, and check the **Use Passive FTP [for firewall and DSL modem compatibility]** check box.

Step 4 Click **OK** to save changes.

Using Passive FTP to Access and Download the MIB Files

To access MIB files using passive FTP, you must know the names of the MIB files that you want to download. See "Using HTTP to Access and Download the MIB Files from CCO" section on page 7 to access the Cisco MDS 9000 Family support list for the names of supported MIBs. These steps assume that your passive FTP utility has UNIX-like commands.

To download MIB files with passive FTP, follow these steps:

Step 1 Access ftp.cisco.com using passive FTP.

Step 2 Log in with your Cisco.com username and password, or as anonymous, with your e-mail address.

Step 3 Enter **cd /pub/mibs/v2/** to change directories.

Step 4 Use the **get** command to copy the desired files to your local system.

Step 5 Use the **quit** command to exit passive FTP.

MIBs, Supported Notifications, RFCs and OIDs Supported by Release in the Cisco MDS 9000 Family

The Cisco MDS 9000 Family supports several standard MIBs and Cisco-specific MIBs. For more information about IETF-standard MIBs in the following tables, refer to http://www.ietf.org. For more information about Cisco-specific MIBS, see the"Cisco-Specific MIBs Supported in the Cisco MDS 9000 Family" section on page 16.

The *Cisco MDS 9000 Family MIB Quick Reference Guide* applies to Cisco NX-OS Release 5.0(1a) and earlier Cisco MDS SAN-OS releases.

Note As of NX-OS Release 4.1(1b), SAN-OS has been changed to NX-OS. References to SAN-OS releases before 4.1(1b) still apply.

Table 3 through Table 13 show MIBs that were added to each release from NX-OS Release 5.0(1a) through SAN-OS Release 1.1(x)

Table 2 New MIBs Added to Cisco MDS NX-OS Release 5.2(1)

MIB	Supported Notifications	RFCs	OIDs
CISCO-FCOE-MIB.my			

)

Table 3 New MIBs Added to Cisco MDS NX-OS Release 5.0(1a)

MIB	Supported Notifications	RFCs	OIDs
CISCO-SYSTEM-EXT-MIB	cseHaRestartNotify		1.3.6.1.4.1.9.9.305.1.3.5.0.1
	cseShutDownNotify		1.3.6.1.4.1.9.9.305.1.3.5.0.2
	cseFailSwCoreNotify		1.3.6.1.4.1.9.9.305.1.4.3.0.1
	cseFailSwCoreNotifyExtended		1.3.6.1.4.1.9.9.305.1.4.3.0.2
	ciscoSwFailureNotifEnable		1.3.6.1.4.1.9.9.305.1.5.1
CISCO-CONFIG-MAN-MIB	ccmHistoryRunningLastChanged		1.3.6.1.4.1.9.9.43.2.0.2

Table 4 New MIBs Added to Cisco MDS NX-OS Release 4.2(1)

MIB	Supported Notifications	RFCs	OIDs
CISCO-CALLHOME-MIB	ccmSmtpMsgSendFailNotif		1.3.6.1.4.1.9.9.300.0.4
	ccmEventNotif		1.3.6.1.4.1.9.9.300.0.5
CISCO-SAN-BASE-SVC-MIB	ciscoSanBaseSvcInterfaceCreate		1.3.6.4.1.9.9.702.0.1
	ciscoSanBaseSvcInterfaceDelete		1.3.6.4.1.9.9.702.0.2
	ciscoSanBaseSvcClusterNewMaster		1.3.6.4.1.9.9.702.0.2
CISCO-NOTIFICATION-CONTROL-MIB			
CISCO-VLAN-Membership-MIB	vtpVlanName		1.3.6.1.4.1.9.9.46.1.3.1.1.4
CISCO-ENTITY-FRU-CONTROL-MIB	cefcModuleStatusChange		1.3.6.1.4.1.9.9.117.2.0.1
	cefcPowerStatusChange		1.3.6.1.4.1.9.9.117.2.0.2
	cefcFRUInserted		1.3.6.1.4.1.9.9.117.2.0.3
	cefcFRURemoved		1.3.6.1.4.1.9.9.117.2.0.4
	cefcUnrecognizedFRU		1.3.6.1.4.1.9.9.117.2.0.5
	cefcFanTrayStatusChange		1.3.6.1.4.1.9.9.117.2.0.6
	cefcPowerSupplyOutputChange		1.3.6.1.4.1.9.9.117.2.0.7
FCMGMT-MIB	connUnitPortStatusChange		1.3.6.1.3.94.0.6
	connUnitStatusChange		1.3.6.1.3.94.0.1
Note: We support draft version of FCMGMT-MIB			

=

Table 5 New MIBs Added to Cisco MDS NX-OS Release 4.1(3)

MIB	Supported Notifications	RFC	OIDs
CISCO-NOTIFICATION-LOG-CAPABILITY			
CISCO-ENTITY-VENDORTYPE-OID-MIB			1.3.6.1.4.1.9.12.3
CISCO-CONFIG-MAN-MIB.my	ccmCLIRunningConfig Changed		1.3.6.1.4.1.9.9.43.2.0.2

Table 6 New MIBs Added to Cisco MDS NX-OS Release 4.1(1b)

MIB	Supported Notifications	RFCs	OIDs
CISCO-ENTITY-DISPLAY-MIB			
CISCO-NPORT-VIRTUALIZATION-MIB.my			
CISCO-IF-EXTENSION-MIB.my	cieDelayedLinkUpDownNotify		1.3.6.1.4.1.9.9.276
	cieLinkDown		.1.3.6.1.4.1.9.9.276.0.1
	cieLinkUp		.1.3.6.1.4.1.9.9.276.0.2

Table 7 New MIBs Added to Cisco MDS SAN-OS Release 2.0(2b)

MIB	Supported Notifications	RFCs	OIDs
CISCO-SCSI-FLOW-MIB			
CISCO-SSM-PROV-MIB			

Table 8 New MIBs Added to Cisco MDS SAN-OS Release 2.0(1b)

MIB	Supported Notifications	RFCs	OIDs
CISCO-CALLHOME-CAPABILITY			
CISCO-CFS-MIB	ciscoCFSFeatureActionNotify	Note: The following groups from this MIB are supported: cfsFeatureAction NotifiGroup cfsMargeFailNoti fGroup cfsPeerDiscovery NotifGroup	.1.3.6.1.4.1.9.9.433.0.1
	ciscoCFSMergeFailNotify		.1.3.6.1.4.1.9.9.433.0.2
	ciscoCFSDiscoveryCompleteNotify		.1.3.6.1.4.1.9.9.433.0.3
CISCO-DNS-CLIENT-CAPABILITY			
CISCO-DNS-CLIENT-MIB			
CISCO-DYNAMIC-PORT-VSAN-MIB			
CISCO-ENHANCED-IPSE-MIB			
CISCO-FC-DEVICE-ALIAS-MIB			
CISCO-FC-MULTICAST-MIB			
CISCO-IETF-ISNS-MGMT-CAPABILITY			
CISCO-IETF-ISNS-MGMT-MIB	cIsnsServerStart		.1.3.6.1.4.1.9.10.116.1.3.0.1
	cIsnsServerShutdown		.1.3.6.1.4.1.9.10.116.1.3.0.2
CISCO-IKE-CONFIGURATION-MIB			
CISCO-IKE-FLOW-EXT-MIB			
CISCO-IKE-FLOW-MIB			
CISCO-IPSEC-PROVISIONING-MIB			
CISCO-IPSEC-SIGNALING-MIB			
CISCO-IPSEC-TC			
CISCO-ISNS-IP-NW-DISCOVERY-MIB			

Table 8 New MIBs Added to Cisco MDS SAN-OS Release 2.0(1b) (continued)

MIB	Supported Notifications	RFCs	OIDs
CISCO-PORT-TRACK-MIB			
CISCO-SNMP-VACM-EXT-MIB			
CISCO-ZS-EXT-MIB	czseZoneTechniqueChangeNotify		.1.3.6.1.4.1.9.9.427.0.1

Table 9 New MIBs Added Since Cisco MDS SAN-OS Release 1.3(x)

MIB	Supported Notifications	RFCs	OIDS
CISCO-DIFFSERV-EXT-MIB			
CISCO-FCC-MIB	ciscoFCCCongestionStateChange		.1.3.6.1.4.1.9.9.365.0.1
	ciscoFCCCongestionRateLimitStart		.1.3.6.1.4.1.9.9.365.0.2
	ciscoFCCCongestionRateLimitEnd		.1.3.6.1.4.1.9.9.365.0.3
CISCO-FCSP-MIB			
CISCO-FCTRACEROUTE-MIB	fcTraceRouteCompletionNotify		.1.3.6.1.4.1.9.9.296.1.3.0.1
CISCO-FDMI-MIB	cfdmiRejectRegNotify		.1.3.6.1.4.1.9.9.373.0.1
CISCO-FEATURE-CONTROL-MIB	ciscoFeatureOpStatusChange	Note: The following groups from this MIB are supported: cfcFeatureGroup cfcNotificationGroup	.1.3.6.1.4.1.9.9.377.0.1
CISCO-ISNS-CLIENT-MIB			
CISCO-IVR-MIB		Note: The following groups from this MIB are supported: civrPfcidGroup civrZoneScalabilityGroup civrScalabilityNotificationGroup civrStatusGroup civrNotificationGroup	civrZoneActivationDoneNotify civrZoneDeactivationDoneNotify civrDomainConflictNotify civrZoneCompactNotify civrAfidConfigNotify
CISCO-SECURE-SHELL-MIB			
CISCO-SVC-INTERFACE-MIB	csiWarningTrap		.1.3.6.1.4.1.9.9.378.2.0.2
	csiInformationTrap		.1.3.6.1.4.1.9.9.378.2.0.3

Table 10 MIBs Added in Cisco MDS SAN-OS Release 1.3(1)

MIB	Supported Notifications	RFCs	OIDs
CISCO-AAA-SERVER-CAPABILITY			
CISCO-AAA-SERVER-EXT-CAPABILTIY			
CISCO-AAA-SERVER-EXT-MIB			
CISCO-AAA-SERVER-MIB	casServerStateChange		1.3.6.1.4.1.9.10.56.2.0.1
CISCO-FICON-MIB			
CISCO-VIRTUAL-NW-IF-MIB	virtualNwIfCreateEntryNotify		.1.3.6.1.4.1.9.9.290.1.3.0.1
	virtualNwIfDeleteEntryNotify		.1.3.6.1.4.1.9.9.290.1.3.0.2

Table 11 New MIBs Added to Cisco MDS SAN-OS Release 1.2(x) (continued)

MIB	Supported Notifications	RFCS	OIDs
CISCO-COMMON-ROLES-MIB			
CISCO-DM-MIB	dmDomainIdNotAssignedNotify		.1.3.6.1.4.1.9.9.302.1.3.0.1
	dmNewPrincipalSwitchNotify		.1.3.6.1.4.1.9.9.302.1.3.0.2
	dmFabricChangeNotify		.1.3.6.1.4.1.9.9.302.1.3.0.3
CISCO-ENTITY-VENDOR-OID-MIB			
CISCO-FC-FE-MIB	fcTrunkIfDownNotify		.1.3.6.1.4.1.9.9.289.1.3.0.1
	fcTrunkIfUpNotify		.1.3.6.1.4.1.9.9.289.1.3.0.2
	fclfElpReject		.1.3.6.1.4.1.9.9.289.1.3.0.3
	fcotInserted		.1.3.6.1.4.1.9.9.289.1.3.0.4
	fcotRemoved		.1.3.6.1.4.1.9.9.289.1.3.0.5
CISCO-FC-SPAN-MIB			
CISCO-FCIP-MGMT-EXT-MIB			
CISCO-FCIP-MGMT-MIB			
CISCO-IMAGE-MIB			
CISCO-IMAGE-UPGRADE-MIB	ciuUpgradeOpCompletionNotify		.1.3.6.1.4.1.9.9.360.0.1
CISCO-IP-PROTOCOL-FILTER-MIB			
CISCO-ISCI-GW-MIB			
CISCO-LICENSE-MGR-MIB	clmLicenseExpiryNotify		1.3.6.1.4.1.9.9.369.3.0.1
	clmNoLicenseForFeatureNotify		1.3.6.1.4.1.9.9.369.3.0.2
	clmLicenseFileMissingNotify		1.3.6.1.4.1.9.9.369.3.0.3
	clmLicenseExpiryWarningNotify		1.3.6.1.4.1.9.9.369.3.0.4
CISCO-NTP-MIB			
CISCO-PORT-CHANNEL-MIB			

Table 11 New MIBs Added to Cisco MDS SAN-OS Release 1.2(x) (continued)

MIB	Supported Notifications	RFCS	OIDs
CISCO-PSM-MIB	ciscoPsmPortBindFPortDenyNotify	The following groups from this MIB are supported: ciscoPsmPortBindNotifyGroup ciscoPsmFabricBindNotifyGroup ciscoPsmFabricBindNotifyGroupR1	.1.3.6.1.4.1.9.9.364.0.1
	ciscoPsmPortBindEPortDenyNotify		.1.3.6.1.4.1.9.9.364.0.2
	ciscoPsmFabricBindDenyNotifyNew		.1.3.6.1.4.1.9.9.364.0.4
CISCO-PSM-MIB-CAPABILITY		ciscoPsmPortBindFPortDenyNotify ciscoPsmPortBindEPortDenyNotify ciscoPsmFabricBindDenyNotify ciscoPsmFabricBindDenyNotifyNew	
CISCO-VSAN-MIB	vsanStatusChange		.1.3.6.1.4.1.9.9.282.1.3.0.1
CISCO-ZS-MIB	zoneServiceReqRejNotify		.1.3.6.1.4.1.9.9.294.1.4.0.1
	zoneMergeFailureNotify		.1.3.6.1.4.1.9.9.294.1.4.0.2
	zoneMergeSuccessNotify		.1.3.6.1.4.1.9.9.294.1.4.0.3
	zoneDefZoneBehaviourChngNotify		.1.3.6.1.4.1.9.9.294.1.4.0.4
	zoneUnsuppMemInIntOpModeNotify		.1.3.6.1.4.1.9.9.294.1.4.0.5
	zoneActivateNotify		.1.3.6.1.4.1.9.9.294.1.4.0.6
	zoneCompactNotify		.1.3.6.1.4.1.9.9.294.1.4.0.7

Table 12 Standard MIBs Supported by Cisco MDS SAN-OS Release 1.1(x)

MIB	Supported Notifications	Comment	OIDs
ENTITY-MIB	entConfigChange	RFC 2737 Note: The following groups from this MIB are supported: entityPhysicalGroup entityPhysical2Group entityGeneralGroup entityNotificationsGroup	.1.3.6.1.2.1.47.2.0.1
ETHERLIKE-MIB		RFC 2665	
FIBRE-CHANNEL-FE-MIB		RFC 2837	
IF-MIB	linkDown	RFC 2863	.1.3.6.1.6.3.1.1.5.3
	linkUp		.1.3.6.1.6.3.1.1.5.4
INET-ADDRESS-MIB		RFC 3291	
IP-FORWARD-MIB		RFC 2096	
IP-MIB		RFC 2011	

Table 12 Standard MIBs Supported by Cisco MDS SAN-OS Release 1.1(x) (continued)

MIB	Supported Notifications	Comment	OIDs
NOTIFICATION-LOG-MIB		RFC 3014	
RMON-MIB	risingAlarm	RFC 2819	.1.3.6.1.2.1.16.0.1
	fallingAlarm	Note: The following groups from this MIB are supported: rmonAlarmGroup rmonEventGroup rmonNotificationGroup	.1.3.6.1.2.1.16.0.2
SNMP-COMMUNITY-MIB		RFC 2576	
SNMP-FRAMEWORK-MIB		RFC 2571	
SNMP-NOTIFICATION-MIB.		RFC 3413	
SNMP-TARGET-MIB		RFC 3413	
SNMP-USM-MIB		RFC 2574 **Note** Referred to as SNMP-USER-BASED-SM-MIB in RFC 2574.	
SNMP-VACM-MIB		RFC 2575 **Note** Referred to as SNMP-VIEW-BASED-ACM-MIB in RFC 2575.	
SNMPv2-MIB	coldStart	RFC 1907	.1.3.6.1.6.3.1.1.5.1
	warmStart		.1.3.6.1.6.3.1.1.5.2
	authenticationFailure		.1.3.6.1.6.3.1.1.5.5
TCP-MIB		RFC 2012	
UDP-MIB		RFC 2013	
VRRP-MIB		RFC 2787	

Table 13 Cisco-Specific MIBs Supported by Cisco MDS SAN-OS Release 1.1(x)

MIB	Supported Notifications	RFCs	OIDs
CISCO-CALLHOME-MIB	ccmSmtpServerFailNotif		.1.3.6.1.4.1.9.9.300.0.1
	ccmAlertGroupTypeAddedNotif		.1.3.6.1.4.1.9.9.300.0.2
	ccmAlertGroupTypeDeletedNotif		.1.3.6.1.4.1.9.9.300.0.3
CISCO-CONFIG-COPY-MIB	ccCopyCompletion		.1.3.6.1.4.1.9.9.96.2.1.1
CISCO-ENTITY-ASSET-MIB			
CISCO-ENTITY-EXT-MIB			
CISCO-ENTITY-FRU-CONTROL-MIB	cefcModuleStatusChange		.1.3.6.1.4.1.9.9.117.2.0.1
	cefcPowerStatusChange		.1.3.6.1.4.1.9.9.117.2.0.2
	cefcFRUInserted		.1.3.6.1.4.1.9.9.117.2.0.3
	cefcFRURemoved		.1.3.6.1.4.1.9.9.117.2.0.4
	cefcUnrecognizedFRU		.1.3.6.1.4.1.9.9.117.2.0.5

Table 13 Cisco-Specific MIBs Supported by Cisco MDS SAN-OS Release 1.1(x) (continued)

MIB	Supported Notifications	RFCs	OIDs
	cefcFanTrayStatusChange		.1.3.6.1.4.1.9.9.117.2.0.6
CISCO-ENTITY-SENSOR-MIB	entSensorThresholdNotification		.1.3.6.1.4.1.9.9.91.2.0.1
CISCO-EXT-SCSI-MIB	ciscoExtScsiLunDiscDoneNotify		.1.3.6.1.4.1.9.9.299.1.2.0.1
CISCO-FC-ROUTE-MIB			
CISCO-FCPING-MIB	fcPingCompletionNotify		.1.3.6.1.4.1.9.9.295.1.3.0.1
CISCO-FCS-MIB	fcsReqRejNotify		.1.3.6.1.4.1.9.9.297.1.4.0.1
	fcsDiscoveryCompleteNotify		.1.3.6.1.4.1.9.9.297.1.4.0.2
	fcsMgmtAddrChangeNotify		.1.3.6.1.4.1.9.9.297.1.4.0.3
CISCO-FLASH-MIB			
CISCO-FSPF-MIB	fspfNbrStateChangeNotify		.1.3.6.1.4.1.9.9.287.3.0.1
CISCO-HC-ALARM-MIB	cHcRisingAlarm		.1.3.6.1.4.1.9.10.93.2.0.1
	cHcFallingAlarm		.1.3.6.1.4.1.9.10.93.2.0.2
CISCO-IF-EXTENSION-MIB			
CISCO-IMAGE-MIB			
CISCO-IP-IF-MIB			
CISCO-ISCSI-MIB			
CISCO-NS-MIB	fcNameServerRejectRegNotify		.1.3.6.1.4.1.9.9.293.1.4.0.1
	fcNameServerDatabaseFull		.1.3.6.1.4.1.9.9.293.1.4.0.2
	fcNameServerEntryAdd		.1.3.6.1.4.1.9.9.293.1.4.0.3
	fcNameServerEntryDelete		.1.3.6.1.4.1.9.9.293.1.4.0.4
CISCO-PROCESS-MIB			
CISCO-RADIUS-MIB			
CISCO-RF-MIB	ciscoRFSwactNotif		.1.3.6.1.4.1.9.9.176.2.0.1
CISCO-RF-SUPPLEMENTAL-MIB			
CISCO-RMON-CONFIG-MIB			
CISCO-RSCN-MIB	rscnElsRejectReqNotify		.1.3.6.1.4.1.9.9.292.1.4.0.1
	rscnIlsRejectReqNotify		.1.3.6.1.4.1.9.9.292.1.4.0.2
CISCO-SCSI-MIB			
CISCO-SMI			
CISCO-STTC			
CISCO-SYSLOG-EXT-MIB	clogMessageGenerated		.1.3.6.1.4.1.9.9.41.2.1
CISCO-SYSTEM-EXT-MIB	ciscoSystemClockChanged		.1.3.6.1.4.1.9.9.131.2.1
CISCO-TC			
CISCO-WWNMGR-MIB.my	wwnmType1WwnShortageNotify		.1.3.6.1.4.1.9.9.286.1.2.1.0.1
	wwnmType1WwnAvailableNotify		.1.3.6.1.4.1.9.9.286.1.2.1.0.2
	wwnmTypeOtherWwnShortageNotify		.1.3.6.1.4.1.9.9.286.1.2.1.0.3
	wwnmTypeOtherWwnAvailableNotify		.1.3.6.1.4.1.9.9.286.1.2.1.0.4

Cisco-Specific MIBs Supported in the Cisco MDS 9000 Family

This section describes the Cisco-specific MIBs that are supported by latest Cisco MDS NX-OS and SAN-OS release for the Cisco MDS 9000 Family of multilayer directors and fabric switches. The Cisco-specific MIBs are listed in alphabetical order.

- CISCO-AAA-SERVER-EXT-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-CALLHOME-MIB
- CISCO-CALLHOME-CAPABILITY
- CISCO-CDP-MIB
- CISCO-CFS-MIB
- CISCO-COMMON-MGMT-MIB
- CISCO-COMMON-MGMT-CAPABILITY
- CISCO-COMMON-ROLES-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIGMAN-MIB
- CISCO-DIFFSERV-EXT-MIB
- CISCO-DIFFSERV-MIB-CAPABILITY
- CISCO-DM-MIB
- CISCO-DNS-CLIENT-MIB
- CISCO-DYNAMIC-PORT-VSAN-MIB
- CISCO-ENHANCED-IPSEC-FLOW-MIB
- CISCO-ENHANCED-IPSEC-FLOW-CAPABILITY
- CISCO-ENTITY-ASSET-MIB
- CISCO-ENTITY-DISPLAY-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-FRU-CONTROL-CAPABILITY
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDOR-OID-MIB
- CISCO-EXT-SCSI-MIB
- CISCO-FC-DEVICE-ALIAS-MIB
- CISCO-FC-FE-MIB
- CISCO-FC-MULTICAST-MIB
- CISCO-FC-MGMT-MIB
- CISCO-FC-ROUTE-MIB
- CISCO-FC-SDV-MIB
- CISCO-FC-SPAN-MIB

- CISCO-FCC-MIB
- CISCO-FCIP-MGMT-EXT-MIB
- CISCO-FCIP-MGMT-MIB
- CISCO-FCOE-MIB
- CISCO-FCPING-MIB
- CISCO-FCS-MIB
- CISCO-FCSP-MIB
- CISCO-FCTRACEROUTE-MIB
- CISCO-FDMI-MIB
- CISCO-FDMI-CAPABILITY
- CISCO-FEATURE-CONTROL-MIB
- CISCO-FICON-MIB
- CISCO-FLASH-MIB
- CISCO-FLEXATTACH-MIB
- CISCO-FSPF-MIB
- CISCO-HC-ALARM-MIB
- CISCO-IETF-IP-FORWARD-MIB
- CISCO-IETF-ISNS-MGMT-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IKE-CONFIGURATION-MIB
- CISCO-IKE-FLOW-EXT-MIB
- CISCO-IKE-FLOW-EXT-CAPABILITY
- CISCO-IKE-FLOW-MIB
- CISCO-IKE-FLOW-CAPABILITY
- CISCO-IMAGE-CHECK-MIB
- CISCO-IMAGE-MIB
- CISCO-IMAGE-UPGRADE-MIB
- CISCO-INTERFACE-XCVR-MONITOR-MIB
- CISCO-IP-IF-MIB
- CISCO-IP-NW-DISCOVERY-MIB
- CISCO-IP-NW-DISCOVERY-CAPABILITY
- CISCO-IP-PROTOCOL-FILTER-MIB
- CISCO-IPSEC-PROVISIONING-MIB
- CISCO-IPSEC-PROVISIONING-CAPABILITY
- CISCO-IPSEC-SIGNALING-MIB
- CISCO-IPSEC-TC
- CISCO-ISCI-GW-MIB
- CISCO-ISCSI-MIB

- CISCO-ISNS-CLIENT-MIB
- CISCO-ISNS-IP-NW-DISCOVERY-MIB
- CISCO-IVR-MIB
- CISCO-IVR-CAPABILITY
- CISCO-LICENSE-MGR-MIB
- CISCO-LICENSE-MGR-CAPABILITY
- CISCO-NOTIFICATION-CONTROL-MIB
- CISCO-NOTIFICATION-LOG-CAPABILITY
- CISCO-NS-MIB
- CISCO-NTP-MIB
- CISCO-NPORT-VIRTUALIZATION-MIB
- CISCO-PORT-CHANNEL-MIB
- CISCO-PORT-CHANNEL-CAPABILITY
- CISCO-PORT-TRACK-MIB
- CISCO-PREFERRED-PATH-MIB
- CISCO-PROCESS-MIB
- CISCO-PSM-MIB
- CISCO-RADIUS-MIB
- CISCO-RF-MIB
- CISCO-RF-SUPPLEMENTAL-MIB
- CISCO-RMON-CONFIG-MIB
- CISCO-RSCN-MIB
- CISCO-SAN-BASE-SVC-MIB
- CISCO-SANTAP-MIB
- CISCO-SCSI-FLOW-MIB
- CISCO-SCSI-MIB
- CISCO-SECURE-SHELL-MIB
- CISCO-SME-MIB
- CISCO-SMI
- CISCO-SNMP-VACM-EXT-MIB
- CISCO-SSM-PROV-MIB
- CISCO-ST-TC
- CISCO-SVC-INTERFACE-MIB
- CISCO-SYSLOG-EXT-MIB
- CISCO-SYSLOG-MIB
- CISCO-SYSTEM-MIB
- CISCO-SYSTEM-EXT-MIB
- CISCO-TC

- CISCO-TPC-MIB
- CISCO-VIRTUAL-NW-IF-MIB
- CISCO-VSAN-MIB
- CISCO-VSAN-CAPABILITY
- CISCO-WWNMGR-MIB
- CISCO-ZS-EXT-MIB
- CISCO-ZS-MIB

CISCO-AAA-SERVER-EXT-MIB

This MIB extension enhances the casConfigTable of the CISCO-AAA-SERVER-MIB to include other types of server addresses. It also manages the following:

- Generic configurations as applied on the Authentication, Authorization, and Accounting (AAA) module.
- Global configuration settings; that is, settings for all the AAA servers instrumented in one instance of this MIB.
- AAA server group configuration.
- Application-to-AAA function-to-server group mapping configuration.

CISCO-AAA-SERVER-EXT-CAPABILTIY

The CISCO-AAA-SERVER-EXT-CAPABILITY provides the implementation details for the CISCO-AAA-SERVER-EXT-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-AAA-SERVER-MIB

This MIB provides configuration and statistics reflecting the state of an AAA server operation within the device and AAA communications with external servers. The CISCO-AAA-SERVER-MIB provides the following information:

- A table for configuring AAA servers.
- Identities of external AAA servers.
- Distinct statistics for each AAA function.
- Status of servers providing AAA functions.

A server is defined as a logical entity that provides any of the three AAA functions. A TACACS+ server consists of all three functions with a single IP address and a single TCP port. A RADIUS server consists of the authentication and accounting pair with a single IP address but distinct UDP ports, or it may be either authentication or accounting. It is possible to have two distinct RADIUS servers at the same IP address, one providing authentication only, and the other accounting only. This MIB replaced CISCO-RADIUS-MIB in Cisco MDS NX-OS or SAN-OS Release 1.3 and later.

CISCO-AAA-SERVER-CAPABILITY

The CISCO-AAA-SERVER-CAPABILITY provides the implementation details for the CISCO-AAA-SERVER-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-SAN-BASE-SVC-MIB

This MIB manages service in the Storage Area Network (SAN). Service is deployed on service nodes on multiple switches forming a cluster. Nodes in the same cluster take on the workload of a failed node to provide fault tolerance. An example of service that can be deployed is I/O Acceleration (IOA) service.

CISCO-CALLHOME-MIB

This MIB manages the Call Home feature. Customers deploying storage solutions to run mission critical applications demand very high availability and serviceability from their products and support partners. To meet these requirements, Call Home allows the storage system experiencing hardware or software problems to automatically send the relevant failure information back to the support center for troubleshooting or to get replacement hardware dispatched. Call Home also provides advanced features that allow storage systems to send performance, accounting, and system health information in addition to the fault information.

CISCO-CALLHOME-CAPABILITY

The CISCO-CALLHOME-CAPABILITY provides the implementation details for the CISCO-CALLHOME-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-CDP-MIB

CDP is a device discovery protocol that runs on all Cisco manufactured equipment (that is routers, bridges, communication servers, WBU switches). Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

The CISCO-CDP-MIB provides information about the device identifications, CDP running status, CDP transmitting frequency, and the time for the receiving device to hold CDP messages (time to live). This MIB stores information in a table called cdpGlobalInfo.

CISCO-CFS-MIB

This MIB facilitates the global level control over the CFS capable features in the system. This MIB applies to one or more sets of devices that have connectivity through the SAN fabric. Many features in the Cisco MDS 9000 Family need to exchange information between peer devices across the SAN fabric. CFS provides this general mechanism for data and configuration distribution within the fabric.

A feature supported in a device may or may not be CFS capable. In case a feature is CFS capable, the control of the CFS operations are instrumented through this MIB. As part of the CFS configuration, you must enable the feature for data distribution on all peer devices. The CFS, in addition to providing the basic distribution infrastructure to the CFS capable features in a stable fabric, also provides the infrastructure to handle data distribution when two stable fabrics merge.

CISCO-COMMON-MGMT-MIB

This MIB integrates different elements of managing a device. For example, different device access methods (such as CLI, SNMP, XML, and others) have different sets of users who are accustomed to communicating with the device. The ccmCommonUserTable provides the framework in which to create one set of users that is common across all the device access methods.

This framework integrates the management of different access methods.

CISCO-COMMON-MGMT-CAPABILITY

The CISCO-COMMON-MGMT-CAPABILITY provides the implementation details for the CISCO-COMMON-MGMT-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-COMMON-ROLES-MIB

This MIB manages the common roles between access methods, such as the CLI, SNMP, and XML interfaces. Every user on a device is associated with a role. A user role defines access rights afforded to the users that belong to this role. A role specifies which commands or operations a user can perform on which information.

This MIB describes a framework in which a role is defined independent of access methods. It is up to the particular access method to convert this framework information into native information. For example, SNMP needs to convert common role framework to VACM.

Note that this framework could also be used for access methods other than SNMP, XML, and CLI.

The framework needs a list of features and a list of operations they can support. The features provide the data context and are system dependent. The operations are the actions that can be performed on the data. The roles are defined in terms of rules. The rules are essentially access rights that specify whether or not a certain operation is permitted on a feature.

CISCO-CONFIG-COPY-MIB

This MIB facilitates copying configuration files for a Cisco MDS 9000 Family switch in the following ways:

- Copying running or startup configurations to or from the network (using a protocol such as TFTP, FTP, SCP, or SFTP).
- Copying running configurations to startup configurations and vice versa.
- Copying a running or startup configuration to a file on the local Cisco MDS NX-OS or SAN-OS file system and vice versa.

CISCO-CONFIGMAN-MIB

This 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. This MIB notification indicates that the running configuration of the managed system has changed from the CLI. If the managed system supports a separate configuration mode (where the configuration commands are entered under a

configuration session that affects the running configuration of the system), then this notification is sent when the configuration mode is exited. During this configuration session there can be one or more running configuration changes.

CISCO-DIFFSERV-EXT-MIB

This MIB extension to DIFFSERV-MIB (RFC 3289) defines a Fibre Channel multifield filter to be used in conjunction with DIFFSERV-MIB. It also helps in associating differentiated services classifiers to interfaces on a VSAN through the cdsmDataPathTable defined in this MIB.

CISCO-DIFFSERV-MIB-CAPABILITY

The CISCO-DIFFSERV-MIB-CAPABILITY provides the implementation details for the CISCO-DIFFSERV-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-DM-MIB

This MIB is for the domain management functionality defined by the Fibre Channel standards (FC-SW2). For the purposes of this MIB, Domain Manager (DM) is the software functionality that executes in both the principal switch and in other switches. This MIB contains DM-related parameters that can be configured and monitored for each of the VSANs configured on this switch.

CISCO-DNS-CLIENT-MIB

This MIB provides configuration for a Domain Name Service (DNS) client, which includes the ability to add or remove DNS servers and configure the domain name options for the local entity.

CISCO-DNS-CLIENT-CAPABILITY

The CISCO-DNS-CLIENT-CAPABILITY provides the implementation details for the CISCO-DNS-CLIENT-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-DYNAMIC-PORT-VSAN-MIB

This MIB manages the DPVM feature. DPVM assigns VSANs dynamically to switch ports based on the device logging in to the port. This device can be identified by its port world wide name (pWWN) and/or its node world wide name (nWWN).

CISCO-ENHANCED-IPSEC-FLOW-MIB

This MIB monitors IP Security (IPsec-based) networks. The MIB contains four major groups of objects that are used to manage the IPsec protocol. These groups are Phase-2, History, Failure, and Trap Control. The Phase-2 group pertains to IPsec data tunnels. The History group aids applications that do trending analysis. The Failure group provides troubleshooting and debugging of the VPN router. This MIB includes counters that detect potential security violations.

CISCO-ENHANCED-IPSEC-FLOW-CAPABILITY

The CISCO-ENHANCED-IPSEC-FLOW-CAPABILITY provides the implementation details for the CISCO-ENHANCED-IPSEC-FLOW-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-ENTITY-DISPLAY-MIB

This MIB object provides information about the status of display devices such as LEDs and alphanumeric displays which, are present on the physical entities contained by the managed system. The MIB objects indicate the color currently seen on the displays specified in this entry. If the display specified by this entry is an alphanumeric display that is, the display type is “alphanumeric,” then the color may not apply and this agent may choose to indicate this information by setting this object to ‘‘unknown.”

If the display specified by this entry is an LED display, that is display type is “LCD,” then this object would be an empty string.

The following LED colors are displayed on the Cisco MDS chassis:

- Status LED
- System LED
- Active LED
- Power LED

CISCO-ENTITY-ASSET-MIB

This MIB monitors the asset information of items in the ENTITY-MIB (RFC 2037) entPhysicalTable. This MIB lists the orderable part number, serial number, hardware revision, manufacturing assembly number and revision, firmware ID and revision, if any, and software ID and revision, if any, of relevant entities listed in ENTITY-MIB entPhysicalTable.

Entities that have none of this data available are not listed in this MIB. The table in this MIB is sparse, so some of these variables may not exist for a particular entity at a particular time. For example, a powered-off module does not have a software ID and revision; a power supply would probably never have firmware or software information.

Although the data may have other items encoded in it (for example, a manufacturing date in the serial number), treat all data items as a single string unit. Do not decompose them or parse them. Use only string equals and unequals operations on them.

CISCO-ENTITY-EXT-MIB

This MIB extension to ENTITY-MIB (RFC 2737) contains entities of class module (entPhysicalClass = “module”) that have a processor.

A processor module is defined as a physical entity that has a CPU, RAM, and NVRAM so that it can independently load a bootable image and save a configuration. This MIB provides memory size, memory utilization, and boot image information for these processor modules.

CISCO-ENTITY-FRU-CONTROL-MIB

This MIB extension to ENTITY-MIB (RFC 2737) monitors and configures the operational state of field-replaceable units (FRUs) of the system listed in ENTITY-MIB entPhysicalTable. FRUs include assemblies such as power supplies, fans, processor modules, and interface modules.

CISCO-ENTITY-FRU-CONTROL-CAPABILITY

The CISCO-ENTITY-FRU-CONTROL-CAPABILITY provides the implementation details for the CISCO-ENTITY-FRU-CONTROL-MIB, as implemented in the Cisco MDS NX-OS and SAN-OS.

CISCO-ENTITY-SENSOR-MIB

This MIB extension to ENTITY-MIB (RFC 2737) monitors the values of sensors in ENTITY-MIB entPhysicalTable. Sensors include power meters, temperature gauges, and chassis airflow measurements.

CISCO-ENTITY-VENDOR-OID-MIB

This MIB defines the OIDs that are assigned to various components on Cisco products that are used by the entPhysicalTable of ENTITY-MIB. These OIDs uniquely identify the type of each physical entry.

This MIB assigns OIDs for use as the values of entPhysicalVendorType. The subtrees in which the OID values are assigned are structured into a hierarchy based on the values in ENTITY-MIB (PhysicalClass) textual convention.

CISCO-EXT-SCSI-MIB

This MIB extension to CISCO-SCSI-MIB configures and monitors Small Computer System Interface entities (SCSI entities). SCSI entities include SCSI devices, SCSI targets and initiators, and SCSI ports. This MIB provides vendor and product details for the SCSI entities present in the CISCO-SCSI-MIB.

CISCO-FC-DEVICE-ALIAS-MIB

This MIB provides a configurable name, called a *device alias*, that can be used to reference a device on a Fibre Channel fabric. The device alias is a human-readable name for a world wide name (WWN).

CISCO-FC-FE-MIB

This MIB extension to IF-MIB (RFC 2863) manages Fibre Channel based interfaces and contains all groups from FIBRE-CHANNEL-FE-MIB (RFC 2837) that are relevant to the Cisco fabric. This MIB supports all the port types defined by the textual convention FcPortTypes. In addition, it supports N ports and NL ports.

This MIB supports PortChannel ports. A PortChannel port is a single logical port that contains multiple physical ports as its members.

CISCO-FC-MULTICAST-MIB

This MIB provides configuration for Fibre Channel multicast parameters on any VSAN configured on the local switch. You can set the multicast root mode for any configured VSAN. This MIB works in conjunction with the CISCO-FSPF-MIB.

CISCO-FC-MGMT-MIB

This MIB provides management information specific to Fibre Channel-attached devices. An arbitrary integer value that uniquely identifies this instance among all local Fibre Channel management instances. It is mandatory to keep this value constant between restarts of the agent, and to make every possible effort to keep it constant across restarts althought it is unrealistic to expect it to remain constant across all reconfigurations of the local system across the replacement of all nonvolatile storage.

CISCO-FC-ROUTE-MIB

This MIB configures and displays Fibre Channel routing information. The fcRouteTable contains entries to a destination, sorted by VSAN, output interface, and protocol through which the route was learned. Use fcRoutePreference to select a route when more than one route to the same destination is present in the fcRouteTable. Only entries configured by the user (fcRouteProto = “netmgmt(3)”) can be deleted by the user.

CISCO-FC-SDV-MIB

This MIB manages the Fibre Channel SAN Device Virtualization (SDV) feature on Cisco Fibre Channel devices.

CISCO-FC-SPAN-MIB

This MIB displays and configures switched port analyzer (SPAN) related features in a Fibre Channel device. The SPAN feature enables the user to analyze network traffic by passing traffic from the selected SPAN source port to a SPAN destination (SD) port. A switch probe device attached to the SD port analyzes this traffic. The SPAN feature is nonintrusive and does not affect switching of network traffic for any of the source ports.

CISCO-FCC-MIB

This MIB manages Fibre Channel Congestion Control (FCC). FCC is a Cisco proprietary flow control mechanism that alleviates congestion on Fibre Channel networks. This MIB enables managers to configure the FCC mechanism on the switch, provides statistics on the congestion control, gives notification of congestion state changes of the Fibre Channel port, and monitors the congestion state of the Fibre Channel port.

CISCO-FCIP-MGMT-EXT-MIB

This MIB extension to CISCO-FCIP-MGMT-MIB adds objects that provide additional information about FCIP interfaces not available in the CISCO-FCIP-MGMT-MIB.

CISCO-FCIP-MGMT-MIB

This MIB is the Cisco version of the IETF FCIP MIB draft (draft-ietf-ips-fcip-mib-02.txt). In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding Internet Draft revision. This Cisco MIB was created because of the "subject to change" nature of Internet Drafts. This Cisco MIB may eventually be replaced by a stable RFC.

This MIB manages Fibre Channel over IP (FCIP) devices, monitoring FCIP links and FCIP routing tables.

CISCO-FCOE-MIB

This MIB module is for configuring and monitoring Fibre Channel over Ethernet (FCoE) related entities. This MIB defines the Virtual FC (VFC) Interface as an object that represents either a VF_Port or a VE_Port on the FCF. Virtual FC interfaces can be either statically created or dynamically created at the time of FIP based FLOGI or ELP request.

CISCO-FCPING-MIB

This MIB manages the Fibre Channel ping functionality. Fibre Channel ping mimics IP ping functionality for a Fibre Channel network. This MIB configures a Fibre Channel ping request and displays the Fibre Channel ping results in the fcPingStatsTable.

CISCO-FCS-MIB

This MIB manages a Fabric Configuration Server (FCS). An FCS is defined by the FC-GS3 standard. An FCS always maintains information pertaining to the local switch. However, it typically maintains only limited information on remote topology (remote switch name and corresponding domain ID for each VSAN).

To gather information about the whole topology, set up the desired VSANs in the fcsVsanDiscoveryList objects, and trigger the discovery process. The VSANs that are discovered during this process are selected with fcsVsanDiscoveryList objects. These objects use the FcList textual convention defined in CISCO-ZS-MIB. See the CISCO-ZS-MIB for a complete definition of the bit positions defined with this textual convention. A brief explanation of bit position layout for the fcsVsanDiscoveryList objects follows:

Within the leftmost octet, that is, octet 1 of fcsVsanDiscoveryList2k, the most significant bit represents VSAN 1, the next bit represents VSAN 2 and so on. The least significant bit in octet 256 represents VSAN 2048. The most significant bit in octet 1 of fcsVsanDiscoveryList4k represents VSAN 2049, and the least significant bit of octet 256 in fcsVsanDiscoveryList4k represents VSAN 4096.

Set the bits in the fcsVsanDiscoveryList objects that represent the VSANs you are interested in, and start the discovery process with fcsStartDiscovery. The results populate the other tables in this MIB.

CISCO-FCSP-MIB

This MIB configures and monitors the Fibre Channel Security Protocol (FC-SP). FC-SP defines authentication, authorization, and encryption techniques for the Fibre Channel fabric. Refer to http://www.t11.org for the FC-SP definition.

CISCO-FCTRACEROUTE-MIB

This MIB manages the Fibre Channel trace route functionality. Fibre Channel trace route mimics the IP trace route utility for Fibre Channel fabrics.

CISCO-FDMI-MIB

The Fabric Device Management Interface (FDMI) MIB defines objects for managing devices such as the HBA (host bus adapter). It provides information for devices that have registered with a Fibre Channel fabric using FDMI. For more information about FDMI, refer to *Fibre Channel Generic Services-4 (FC-GS-4)* at http://www.t11.org.

CISCO-FDMI-CAPABILITY

The CISCO-FDMI-CAPABILITY provides the implementation details for the CISCO-FDMI-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-FEATURE-CONTROL-MIB

This MIB enables or disables optional features in the system. Disabling optional features makes the associated feature-specific MIB unavailable. For example, disabling FCIP makes CISCO-FCIP-MIB unavailable. Optional features may require additional configuration beyond the high-level control provided by this MIB. Refer to the associated feature-specific MIB for more configuration requirements. Some optional features may also require a feature license.

CISCO-FICON-MIB

This MIB manages FICON (Fiber Connection), which is an IBM standard transport mechanism for communication between mainframes and devices. The Cisco MDS 9000 Family switches provide the functionality of a FICON director.

CISCO-FLASH-MIB

This MIB configures and monitors flash memory devices on a system. The MIB is organized hierarchically into the following categories:

Device information:

- Device level
- Partition

- File within a partition

Operations:

- Copy
- Partitioning

CISCO-FLEXATTACH-MIB

This MIB enables the automatic generation of virtual WWNs on all of the F port interfaces whose fcIfOperMode is fPort.

The Nx ports register with the Fx ports with a port WWN as indicated by object fcNameServerPortName in the CISCO-NS-MIB. Generally, the Nxports are zoned with other devices which they need to communicate using this port WWN. However, if the device containing Nx port has to be replaced, zoning has to be reconfigured using the port WWN of the new device to eliminate the need for a zoning change, a special WWN is assigned to the corresponding F port and the original port WWN is replaced with this special WWN for any device that is logging through the F port. In addition, the zoning is configured using the special WWN.

CISCO-FSPF-MIB

This MIB configures and monitors the Fabric Shortest Path First (FSPF) parameters on all VSANs configured on the local switch. FSPF is the protocol currently standardized by the T11 committee for routing in Fibre Channel networks. Refer to http://www.t11.org.

CISCO-HC-ALARM-MIB

This MIB defines RMON-MIB(RFC 2819) extensions for high-capacity alarms. This MIB is based on the Internet Draft (draft-ietf-rmonmib-hc-alarm-mib-02.txt). In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding Internet Draft revision. This Cisco MIB was created because of the “subject to change” nature of Internet Drafts. This Cisco MIB eventually maybe replaced by a stable RFC.

This MIB configures RMON alarms that require high-capacity counters (64-bit counters).

CISCO-IETF-IP-FORWARD-MIB

This MIB was extracted from the draft-ietf-ipngwg-rfc2096-update-00.txt. In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding I-D revision. This Cisco MIB is created due to the “subject to change” nature of the I-Ds. This Cisco MIB may later be deprecated, and the stable RFC, which may replace the I-D, may be implemented in its place.

CISCO-IETF-ISNS-MGMT-MIB

This MIB is the Cisco version of the ISNS-MIB from the Internet Draft (draft-ietf-ips-isns-mib-06.txt). In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding Internet Draft revision. This Cisco MIB was created because of the “subject to change” nature of Internet Drafts. This Cisco MIB may eventually be replaced by a stable RFC.

The iSNS protocol provides storage name service functionality on an IP network that is being used for iSCSI or iFCP storage. This MIB configures and monitors iSNS clients and servers, including information about registered objects in an iSNS server.

CISCO-IETF-ISNS-MGMT-CAPABILITY

The CISCO-IETF-ISNS-MGMT-CAPABILITY provides the implementation details for the CISCO-IETF-ISNS-MGMT-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-IETF-VRRP-MIB

This MIB manages Virtual Router Redundancy Protocol (VRRP) over IPv4 and IPv6 protocols. This MIB supports VRRP for IPv4 and IPv6 protocols simultaneously running on a specific interface of a router. This MIB was extracted from the Internet Draft (draft-ietf-vrrp-unified-mib-04.txt).

CISCO-IF-EXTENSION-MIB

This MIB extension to IF-MIB (RFC 2863) adds objects that provide additional information about interfaces not available in other MIBs. This MIB replaces OLD-CISCO-INTERFACES-MIB.

CISCO-IKE-CONFIGURATION-MIB

This MIB provides configuration and monitoring for the IKE. IKE dynamically negotiates security associations between peers and generates keys. IKE may be used with security protocols, such as Fibre Channel Security Protocol (FC-SP) or IPsec, based on the domain of interpretation (DOI).

CISCO-IKE-FLOW-EXT-MIB

This MIB extends the CISCO-IKE-FLOW-MIB, providing additional monitoring objects for IPsec control flows based on the IKE protocol. This MIB monitors the unique identity and type of each peer in an IKE *traffic flow*. For the purposes of this MIB, a traffic flow is a sustained connection between peers used to create security associations (SAs) for either IKE tunnels (ISKAMP SAs) or IPsec tunnels (IPsec SAs).

CISCO-IKE-FLOW-EXT-CAPABILITY

The CISCO-IKE-FLOW-EXT-CAPABILITY provides the implementation details for the CISCO-IKE-FLOW-EXT-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-IKE-FLOW-MIB

This MIB monitors IKE traffic flows. This MIB was extracted from portions of the Internet Draft (draft-ietf-ipsec-flow-monitoring-mib-02.txt). This MIB augments the CISCO-IPSEC-SIGNALING-MIB for IKE-specific entities.

CISCO-IKE-FLOW-CAPABILITY

The CISCO-IKE-FLOW-CAPABILITY provides the implementation details for the CISCO-IKE-FLOW-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-IMAGE-CHECK-MIB

This MIB performs a high availability (HA) compatibility check of different software versions on the active and standby supervisor engines, and it lists any incompatibilities. This MIB uses the following two tables to check the software and list any incompatibilities:

- CiscoImageCheckOpTable—An operations table that invokes a command to check the images.
- CiscoImgChkResultsTable—A read-only table that displays any incompatibilities discovered.

CISCO-IMAGE-MIB

This MIB identifies the capabilities and characteristics of the running image.

CISCO-IMAGE-UPGRADE-MIB

This MIB can upgrade images on modules in the system, show the status of the upgrade operation, and show the type of images that could be run in the system. Examples of modules include a controller card or line card.

The system fills up the ciuImageVariableTable with the type of images the system can support. For performing an upgrade operation, a management application must first read this table and use this information in other tables.

The ciuImageURITable is also filled by the system and provides the image name presently running for each type of image in the system. The user can configure a new image name for each image type as listed in ciuImageVariableTable. The system would use this image on the particular module on the next reboot.

The management application must first determine if an upgrade operation is already in progress in the system by reading the ciuUpgradeOpCommand. If it contains “none,” no other upgrade operation is in progress. Any other value signifies that an upgrade is in progress and a new upgrade operation is not allowed.

Before starting an install, you must first verify version compatibility for the new set of image files (in ciuImageLocInputTable). Set ciuUpgradOpCommand to “check” to compare these new image files to the current system configuration. If ciuUpgradeOpStatus returns “success,” then continue the installation process by setting ciuUpgradOpCommand to “install.”

The tables, ciuVersionCompChkTable, ciuUpgradeImageVersionTable, and ciuUpgradeOpStatusTable, provide the result of the “check” or “install” operation performed using ciuUpgradeOpCommand. These tables are in addition to ciuUpgradeOpStatus, ciuUpgradeOpTimeStarted, ciuUpgradeOpTimeCompleted, and ciuUpgradeOpStatusReason. The ciuUpgradeOpStatus object provides the status of the selected upgrade operation. The user can choose to upgrade only some modules by using ciuUpgradeTargetTable. If this table is empty, then an upgrade operation is performed on all the modules in the system.

CISCO-INTERFACE-XCVR-MONITOR-MIB

This MIB provides the status of the monitoring parameter for a given sensor type in transceiver digital diagnostics on an interface. The value of the monitoring parameter for a given sensor lies are bounded within maximum (high) and minimum (low) limits. If the current value is over the high limit, this status is set to highSet. Upon the value of the sensor coming back into the normal range (between high and low values), this status is set to highClear. Similarly, if the current value is below the low limit, this status is set to lowSet. Upon the value the sensor coming back into normal range subsequently, this

status is set to lowClear. If the current value stays within the high and low limits, this status is set to normal. Also, subsequently after the status had been either highClear or lowClear, if the value is within the high and low limits, this status is set to normal.

CISCO-IP-IF-MIB

This MIB configures IP address characteristics of the interfaces on a device, which includes configuring primary, secondary, and broadcast IP addresses.

CISCO-IP-NW-DISCOVERY-MIB

This MIB provides the ability to initiate, configure, and show discovery results for IP networks in a switch fabric. This MIB replaced CISCO-ISNS-IP-NW-DISCOVER-MIB.

CISCO-IP-NW-DISCOVERY-CAPABILITY

The CISCO-IP-NW-DISCOVERY-CAPABILITY provides the implementation details for the CISCO-IP-NW-DISCOVERY-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-IP-PROTOCOL-FILTER-MIB

This MIB manages information to support packet filtering on IP protocols.

The cippfIpProfileTable allows users to create, delete, and get information about filter profiles. Filter profiles are uniquely identified by the profile names. Filter profiles can be either simple or extended usage types. The usage type cannot be changed once it has been created.

The cippfIfIpProfileTable applies the filtering profiles to device interfaces running IP. A filter profile can be applied to multiple interfaces.

The cippfIpFilterTable contains ordered lists of IP filters for all filtering profiles. Filters and profiles are related if they have the same filter profile name. Filters can be created only if their associated filter profiles already exist in the cippfIpProfileTable. Filters of the same profile name belong to a common profile.

The interface-based cippfIfIpProfileTable can be configured with information independent of the other tables. However, if the profile name in this table matches any profile name in the cippfIpProfileTable and the profile name of any filter entry in the cippfIpFilterTable, the profile is active, and the filter entry is being applied to IP traffic passing through the attached device interfaces. Therefore, any change to the filters in the cippfIpFilterTable or the profile itself in the cippfIpProfileTable affects all the attached interfaces.

CISCO-IPSEC-PROVISIONING-MIB

This MIB provides IPsec configuration in terms of structures specific to the Cisco implementation of IPsec (such as IPsec transforms and crypto maps). It deals with IPsec (Phase-2) configuration only. This MIB may be used to view and provision IPsec-based VPNs.

CISCO-IPSEC-PROVISIONING-CAPABILITY

The CISCO-IPSEC-PROVISIONING-CAPABILITY provides the implementation details for the CISCO-IPSEC-PROVISIONING-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-IPSEC-SIGNALING-MIB

This MIB provides status, performance, and fault detection for a protocol with the generic characteristics of signaling protocols used with IPsec and FC-SP, such as IKE and KINK. Signaling protocols are also referred to in this document as control protocols because they perform session control. The protocol-specific aspects of a signaling protocol are captured in a protocol-specific MIB such as the CISCO-IKE-FLOW-MIB.

This MIB contains major groups of objects that are used to manage the generic aspects of IPsec signaling. These groups include the following information:

- Global statistics, tunnel table, and peer association groups—Aid in real-time monitoring of IPsec signaling activity.
- History group—Aids applications that do trending analysis.
- Failure group—Enables troubleshooting and detection of potential security violations.
- Notifications—Modeled as generic IPsec control notifications and are identified by the specific signaling protocol that caused the notification.

CISCO-IPSEC-TC

This file defines the textual conventions used in the IPsec suite of MIBs, which includes Internet DOI numbers defined in RFC 2407, ISAKMP numbers defined in RFC 2408, and IKE numbers defined in RFC 2409.

CISCO-ISCI-GW-MIB

This MIB configures and monitors iSCSI (SCSI over TCP) gateway functions. An iSCSI node (target or initiator) is presented to the Fibre Channel network as a virtual Fibre Channel node that can be accessed by the real Fibre Channel nodes on that network. Similarly, a Fibre Channel node is presented to the iSCSI network as a virtual iSCSI node that can be access by the real iSCSI nodes on that network. It is up to the gateway implementation how to represent the nodes in each of these networks. For example, a gateway implementation may choose to represent multiple Fibre Channel targets either as one iSCSI target (many to one mapping) or multiple iSCSI targets (one to one mapping).

CISCO-ISCSI-MIB

This MIB manages iSCSI devices and is based on the Internet Draft (draft-ietf-ips-iscsi-mib-05.txt). In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding Internet Draft revision. This Cisco MIB was created because of the "subject to change" nature of Internet Drafts. This Cisco MIB may eventually be replaced by a stable RFC.

The CISCO-ISCSI-MIB is layered between the CISCO-SCSI-MIB and the TCP-MIB (RFC 2012). These MIBs are related as follows:

- CISCO-SCSI-MIB—Each iscsiNode, whether it is an initiator, target, or both, is related to one SCSI device within the CISCO-SCSI-MIB. The iscsiNodeTransportType attribute points to the SCSI transport object within the CISCO-SCSI-MIB, which in turn contains an attribute that points back to the iscsiNode. In this way, a management station can navigate between the two MIBs.
- TCP-MIB—Each iSCSI connection is related to one transport-level connection. The iSCSI connection is related to a TCP connection using its normal (protocol, source address, source port, destination address, and destination port) 5-tuple.

CISCO-ISNS-CLIENT-MIB

This MIB configures and monitors the iSNS client. The Cisco MDS 9000 Family switches act as iSNS clients. This MIB lists iSNS server profiles known to the iSNS client.

CISCO-ISNS-IP-NW-DISCOVERY-MIB

This MIB discovers and manages the *disjoint* IP networks connected to the various Gigabit Ethernet interfaces in the SAN fabric. Disjoint IP networks are separate IP networks that are not reachable to each other using IP. Multiple disjoint IP networks may terminate on a single Fibre Channel switch in a fabric. In such a scenario, the iSNS server must ensure that the targets returned on a query by iSCSI devices are filtered based on access control lists (specified by the user during configuration), and also based on Gigabit Ethernet ports that are reachable by the IP network on which the iSCSI device is present.

The iSNS server partitions all known Gigabit Ethernet ports into disjoint sets based on IP reachability by sending discovery packets. Each discovered set is referred to as an IP network. The Gigabit Ethernet ports contained in these IP networks are referred to as IP network members.

This MIB provides the ability to initiate, configure, and show discovery results for the IP networks in the SAN fabric.

CISCO-IVR-MIB

This MIB manages inter-VSAN routing within the framework of the Cisco inter-VSAN routing (IVR) architecture. IVR allows traffic between VSANs. VSANs are logically separated SANs where traffic does not cross VSAN boundaries. Certain SAN applications need restricted communication between initiators and targets that are in different VSANs. The IVR architecture provides this inter-VSAN communications.

The VSANs logically separate a single physical fabric into multiple logical fabrics. These logical fabrics can be grouped together to form an *autonomous fabric*. In addition to inter-VSAN communication, IVR also enables communication between autonomous fabrics.

CISCO-IVR-CAPABILITY

The CISCO-IVR-CAPABILITY provides the implementation details for the CISCO-IVR-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-LICENSE-MGR-MIB

This MIB manages license files on the system. The Cisco MDS 9000 Family uses licensing to enable advanced features in the product. The licensing model has two options:

- Feature-based licensing—Features that are applicable to the entire switch.
- Module-based licensing—Features that require additional hardware modules.

The license can specify a limit to the number of concurrent uses of the feature, a time limit on the feature, and the device where the feature can be used.

License files are provided to customers when licenses are purchased. Customers should copy the license file to a local computer to allow installation of the license to the switch.

CISCO-LICENSE-MGR-CAPABILITY

The CISCO-LICENSE-MGR-CAPABILITY provides the implementation details for the CISCO-LICENSE-MGR-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-NOTIFICATION-CONTROL-MIB

This MIB provides network management support that regulates the transmission of notifications generated by a system. The system can generate several notifications that pertain to various events. Allowing every notification to transmit may lead to the network being flooded with an excess of network management traffic.

CISCO-NOTIFICATION-LOG-CAPABILITY

The CISCO-NOTIFICATION-LOG-CAPABILITY provides the implementation details for the CISCO-NOTIFICATION-LOG-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-NS-MIB

This MIB manages the name server (NS), which realizes the FC-GS3 requirements for a NS. The NS functionality maintains a database containing the attributes for all hosts and storage devices in each VSAN.

CISCO-NTP-MIB

This MIB monitors an NTP server. The MIB is derived from the *Management of the Network Time Protocol (NTP) with SNMP* publication, Technical Report No. 98-09. Refer to http://www.cis.udel.edu/~sethi/papers/97/ntp-mib-tr.pdf.

NTP is defined in RFC 1309.

CISCO-NPORT-VIRTUALIZATION-MIB

This MIB module manages the N port Virtualization or NPV within the framework of Cisco's

N port virtualization (NPV) architecture. N port virtualization reduces the number of Fibre Channel domain IDs in SANs. Switches operating in the NPV mode do not join a fabric, rather they pass traffic

between NPV core switch links and end devices, which eliminates the domain IDs for these edge switches.

CISCO-PKI-PARTICIPATION-MIB

This MIB organizes the various certificates, key-pairs, and Certificate Authority (CA) related information into SNMP tables.

- The cpkiTrustPointTable—Contains Certificate and CA information.
- The cpkiRSAKeyPairTable—Contains the key-pair information for each key-pair.

An entry in the cpkiTrustPointTable corresponds to a trusted CA that the switch uses to obtain an identity certificate and to verify the peer certificates issued by that CA. The entry contains information about the CA certificate, which includes the following information:

- The identity certificate (if obtained) from the CA.
- The corresponding key-pair from the cpkiTrustPointTable that was used for the identity certificate.
- The information needed for revocation checking of certificates issued by the CA.

The cpkiRSAKeyPairTable contains an entry for each key-pair that is present in the device.

A key-pair entry from the cpkiRSAKeyPairTable can be associated to an entry in the cpkiTrustPointTable. A key-pair entry can be associated to multiple cpkiTrustPointTable entries, but a cpkiTrustPointTable entry is associated with only one key-pair entry.

This MIB supports the certificate work-flow operations used for generating the key pairs and obtaining the certificates for them from various CAs. The following are the steps in one typical workflow:

1. Create a trustpoint (an entry in cpkiTrustPointTable) in the device.
2. Authenticate a CA. (This step involves manually verifying the CA certificate or chain fingerprints and then inputting the CA certificate or chain into the trustpoint.)
3. Generate a keypair (an entry in cpkiRSAKeyPairTable).
4. Associate the keypair to the trustpoint.
5. Generate a pkcs#10 Certificate Signing Request (CSR) in the trustpoint.
6. Submit CSR to the CA and get the identity certificate.
7. Input the identity certificate into the trustpoint.

In another typical certificate workflow, the keypair and the corresponding identity certificate are allowed to be generated or obtained outside of the device by whatever means and then input to the device in the pkcs#12 form.

This MIB does not support configuring individual security services such as SSL, SSH, IPsec and IKE to use particular trustpoints or certificates and key-pairs in them. Instead, the security services certificate usage configuration is supported in the respective feature MIBs.

CISCO-PORT-CHANNEL-MIB

This MIB manages PortChannel ports in the Cisco MDS 9000 Family. In addition to this MIB, CISCO-FC-FE-MIB and IF-MIB (RFC 2863) also contain entries for PortChannel ports. PortChannel refers to the aggregation of multiple physical Fibre Channel ports into one logical port to provide high-aggregated bandwidth, load balancing, and link redundancy.

CISCO-PORT-CHANNEL-CAPABILITY

The CISCO-PORT-CHANNEL-CAPABILITY provides the implementation details for the CISCO-PORT-CHANNEL-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-PORT-TRACK-MIB

This MIB provides configuration for port tracking. Port tracking allows the SAN fabric to recover quickly from *indirect failures* on a port. An indirect failure occurs when a connection fails because of a problem on another link in the path from the port to its remote peer. A *direct failure* occurs when a link failure is detected on the local port. Direct failures implement recovery and redundant port failover more quickly than indirect failures, which are dependent on SAN application timeouts to detect a remote link failure. To speed up recovery times for indirect failures, this MIB marks critical ports as *tracked ports*. Other dependent, or *linked,* ports can be associated with one or more tracked ports. When a tracked port fails, all linked ports are shut down, causing an immediate failover to redundant paths.

CISCO-PREFERRED-PATH-MIB

This MIB provides a method of routing traffic over the selected preferred paths, not necessarily the shortest path, as chosen by routing protocols such as FSPF. This type of control allows you to choose paths based on characteristics, such as frames received on a selected interface or frames with selected source FCID. This feature allows you to ensure path separation between switches for different traffic between a host and a target.

CISCO-PROCESS-MIB

This MIB displays memory and process CPU utilization on Cisco devices. This information should be used as an estimate only.

CISCO-PSM-MIB

This MIB manages the Port Security Manager (PSM). The PSM consists of two aspects: port binding and fabric binding. Port binding is concerned with the security of switch ports, and fabric binding is concerned with the security of the SAN fabric as a whole.

CISCO-PSM-MIB-CAPABILITY

CISCO-PSM-MIB-CAPABILITY provides the implementation details for the CISCO-PSM-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-RADIUS-MIB

This MIB manages the RADIUS server. This MIB was removed in Cisco MDS SAN-OS Release 1.3(1) and replaced by CISCO-AAA-SERVER-MIB.

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 “one -to-one” redundancy on processor cards. RF is not intended to solve all redundancy schemes. RF is not designed to support redundant hardware, such as power supplies.

Redundancy is concerned with the duplication of data elements and software functions to provide an alternative in case of failure. It is a key component to meeting 99.999 percent availability requirements for Class 5 carrier solutions.

In the scope of this MIB definition, peer software elements are redundant and redundant software elements are peers.

CISCO-RF-SUPPLEMENTAL-MIB

This MIB extends CISCO-RF-MIB by providing additional optional status and configuration control for redundant processor platforms.

CISCO-RMON-CONFIG-MIB

This MIB defines configuration extensions for some of the IETF RMON MIBs.

The following terms are used throughout this MIB:

A *SPAN session* is an association of one or more destination(s) with a set of source(s), along with other parameters, to specify the network traffic to be monitored. Each SPAN session is denoted by a unique number.

A *remote SPAN*, also called RSPAN, refers to the analysis of network traffic remotely, from destination port(s) for one or more source ports, distributed in one or more switches in a switched network, through an RSPAN VLAN.

CISCO-RSCN-MIB

Note rscnScrFcId MIB is not supported.

This MIB monitors the Fibre Channel Registered State Change Notification (RSCN) functionality, which is specified by FC-FLA and FC-FS. RSCN is a Fibre Channel service that informs hosts about changes in the fabric. Hosts can receive this information by registering with the fabric controller. This MIB lists which ports are registered for RSCN, and it provides global and per-VSAN statistics on RSCN.

CISCO-SANTAP-MIB

This MIB configures the CVT for the SANTap service on the Fibre Channel switch modules.

SANTap is a Fibre Channel switch-based capability that provides a reliable copy of the data flowing between a set of one or more initiators and a set of one or more targets connected to the fabric.

Administrators must configure the switch to create the CVT for the SANTap service. CVTs are used to implement the control paths that process all SANTap service requests sent out by a device.

CISCO-SCSI-FLOW-MIB

This MIB configures and monitors Small Computer System Interface (SCSI) flows. A SCSI flow is a monitored connection between a SCSI initiator and a SCSI target. The initiator should be connected to a port on the local switch. The target can be present anywhere in the fabric. A SCSI flow is identified uniquely by a SCSI flow ID. The statistics gathered per flow and per LUN include SCSI reads, writes, transmit bytes, receive bytes, transmit frames, and receive frames.

CISCO-SCSI-MIB

This MIB is the Cisco version of the SCSI-MIB from the Internet Draft (draft-ietf-ips-scsi-mib-03.txt). In terms of object syntax and semantics, the content of this Cisco MIB is the same as the corresponding Internet Draft revision. This Cisco MIB was created because of the “subject to change” nature of Internet Drafts. This Cisco MIB may eventually be replaced by a stable RFC.

This MIB configures and monitors SCSI entities. SCSI entities include SCSI devices, SCSI targets and initiators, and SCSI ports.

CISCO-SECURE-SHELL-MIB

This MIB provides management of the SSH protocol. SSH provides secure communications between the network management application and the managed device.

CISCO-SME-MIB

This MIB module manages Storage Media Encryption (SME) service. SME is an encryption service provided by an encryption node residing on a line card in a storage device. It receives clear-text data from the host, encrypts and then sends it to be written to tape or disk. It does the reverse in the opposite direction so the service is completely transparent to the host. The purpose of this service is to enhance data security in case the tape or disk is lost or stolen.

As with any services important the user requires that provides some level of fault tolerance in a graceful manner. SME provides fault tolerance by allowing encryption nodes to be grouped into a cluster. Nodes in the same cluster immediately take over the work of a failed node so that the user does not experience service disruption.

CISCO-SMI

This file gives the Structure of Management Information (SMI) for the Cisco enterprise. A subset of the SMI follows.

ciscoProducts

ciscoProducts is the root object identifier from which sysObjectID values are assigned. Actual values are defined in CISCO-PRODUCTS-MIB.

ciscoAgentCapability

ciscoAgentCapability provides a root object identifier from which AGENT-CAPABILITIES values may be assigned.

ciscoMgmt

ciscoMgmt is the main subtler for new MIB development.

ciscoExperiment

ciscoExperiment provides a root object identifier from which experimental MIBs may be temporarily based. MIBs are typically based here if they fall in one of two categories:

- Cisco versions of IETF Internet Drafts that have not been assigned a permanent object identifier by the IANA.
- Cisco work-in-process MIBs that have not been assigned a permanent object identifier by Cisco, typically because the MIB or technology is experimental.

CISCO-SNMP-VACM-EXT-MIB

This MIB extends the SNMP-VACM-MIB to allow each combination of a securityModel and a securityName to be mapped into additional groupNames. The groups identified by these mappings are in addition to those identified by the vacmGroupName of the vacmSecurityToGroupTable.

CISCO-SSM-PROV-MIB

This MIB provisions features for SSMs. Currently, an SSM has eight data path processors (DPPs), each of which corresponds to four of the 32 ports on the SSM. Each DPP can run a feature independent of the other DPPs. Because the concept of a DPP is transparent to the network manager, groups of ports are used to configure different features. A start port and an end port are specified to identify a DPP and provision a feature.

CISCO-ST-TC

This file defines textual conventions used in MIBs that are specific to SANs in the Cisco MDS 9000 Family.

CISCO-SVC-INTERFACE-MIB

This MIB configures and monitors SVC-related features in SAN switches. SVC supports a virtualized pool of storage from the storage subsystems attached to a SAN. This MIB monitors virtualization features per interface and per VSAN.

CISCO-SYSLOG-EXT-MIB

This MIB configures and monitors system log (syslog) management parameters. Syslog is defined by RFC 3164. Use this MIB to set up syslog servers and set logging severity levels.

CISCO-SYSLOG-MIB

This MIB collects system messages generated by Cisco MDS NX-OS or SAN-OS. These messages are typically sent to a syslog server. Use this MIB to retrieve SYSLOG-MIB system messages.

CISCO-SYSTEM-MIB

This MIB provides Cisco-defined extensions to the MIB-II systemGroup.

CISCO-SYSTEM-EXT-MIB

This MIB monitors high availability (HA) and provides an extension to the SNMP error status when an SNMP **set** request fails.

CISCO-TC

This file defines the common TEXTUAL-CONVENTIONS used in all Cisco MIBs. These conventions make it easier to realize the type or purpose of a MIB object by adding a label to an underlying primitive. *DisplayString* is a frequently used TEXTUAL-CONVENTION defined in SNMP.

CISCO-TPC-MIB

This MIB configures the TPC targets. This MIB is used with the Network Assisted Serverless Backup (NASB) feature. You specify the module and the VSAN on which the TPC feature needs to be configured. Once the feature is configured, target ports are created on the specified module and VSAN that are SCSI Extended Copy (XCOPY) capable. Any application that can source an XCOPY command can use these targets to perform data movement.

TPC derives its name from the fact that there are three entities involved in the process of copying data, either for backup or restore operations. These entities are as follows:

- Entity originating the copy command
- Data source for the copy
- Data destination for the copy

The entity originating the **copy** commands to perform the data transfer can use XCOPY. The TPC feature exposes a disk target with a Logical Unit Number (LUN) 0 that is capable of processing the XCOPY to transfer data from a specified source to a specified destination. On receiving the XCOPY command, the TPC target performs the actual data transfer from the data source to the data destination on behalf of the entity issuing the XCOPY command.

CISCO-VIRTUAL-NW-IF-MIB

This MIB manages virtual network interfaces to VSANs and VLANs. This MIB is used in conjunction with ENTITY-MIB, IF-MIB, CISCO-IF-EXTENSION-MIB, and CISCO-IP-IF-MIB. This MIB monitors the operational status of these virtual network interfaces.

CISCO-VSAN-MIB

This MIB manages VSANs within the framework of the Cisco VSAN architecture. This MIB enables you to create and monitor VSANs. VSANs provide isolation among devices that are physically connected to the same fabric. With VSANs you can create multiple logical SANs over a common physical infrastructure.

CISCO-VSAN-CAPABILITY

The CISCO-VSAN-CAPABILITY provides the implementation details for the CISCO-VSAN-MIB, as implemented in the Cisco MDS NX-OS or SAN-OS.

CISCO-WWNMGR-MIB

This MIB manages the WWN manager functions. The WWN manager on a Cisco MDS 9000 Family switch assigns WWNs to each switch, independent of other WWN managers on other switches. This MIB provides statistics on the limited number of WWNs available to the switch and details on each type of WWN provided.

CISCO-ZS-EXT-MIB

This MIB manages zoning within the framework of the Cisco zone server architecture, which realizes the FC-GS4/SW3 requirements for a zone server. This MIB is an extension to the CISCO-ZS-MIB, which is for managing zoning conforming to FC-GS3/SW2. Refer to http://www.t11.org for the FC-GS4 specification.

GS4/SW3 allows zoning to operate in either basic or enhanced mode of operation. Basic mode is essentially the GS3/SW2 compatible mode (as modeled by CISCO-ZS-MIB). Enhanced mode provides additional capabilities. In enhanced mode of operation, all the configuration should be done within the scope of a session.

CISCO-ZS-MIB

This MIB manages zoning within the framework of the Cisco zone server architecture, which realizes the FC-GS3 requirements for the zone server (ZS). Additionally, the Cisco ZS allows for configuration of LUN zoning, which is an extension to the ZS standard specified by FC-GS3.

Understanding the ENTITY-MIB and Extensions

The ENTITY-MIB provides basic management and identification of physical and logical entities within a network device. Cisco MDS NX-OS snd SAN-OS support for the ENTITY-MIB focuses on the physical entities within a switch or director. This MIB provides details on each module, power supply, and fan tray within a switch chassis. It gives enough information to correctly map the containment of these entities within the switch, building up a chassis view.

Cisco has developed a number of private extensions to the ENTITY-MIB to provide more details for these physical entities. Each of these MIB extensions shares the common index value, entPhysicalIndex, which allows the management application developer to link information across multiple MIBs.

Table 14 lists the Cisco MIB extensions that are linked to the ENTITY-MIB by entPhysical Index.

Table 14 ENTITY-MIB Extensions

MIB	Description
CISCO-ENTITY-ASSET-MIB	Provides manufacturing asset number and revision information per physical entity in the switch.
CISCO-ENTITY-EXT-MIB	Extends the entityPhysicalTable for modules with processors. For each of these modules, this MIB provides memory statistics and LED information.
CISCO-ENTITY-FRU-CONTROL-MIB	Manages field-replaceable units, such as power supplies, fans, and modules.
CISCO-ENTITY-SENSOR-MIB	Provides sensor data for environmental monitors such as temperature gauges.
CISCO-FC-ROUTE-MIB	Provides ingress traffic counters for Fibre Channel, linked to entPhysicalIndex.
CISCO-IMAGE-UPGRADE-MIB	Provides module image management based on entPhysicalIndex.
CISCO-VIRTUAL-NW-IF-MIB	Maps VSAN ID to FC ID and ifIndex, based on entPhysicalIndex.

Extending the IF-MIB

The IF-MIB provides basic management status and control of interfaces and sublayers within a network device. Multiple standard and Cisco-specific MIBs use ifIndex from the IF-MIB to extend management for specific interface types. Cisco MIBs also enhances the two interface notifications, linkUp and linkDown, from the IF-MIB to provide a clearer indication of the reason for these notifications. Cisco MIBs add up to two varbinds to linkUp and linkDown as shown in Table 15.

Table 15 Varibinds added to IF-MIB Notifications

Notification	Varbinds
linkUp	fcIfOperMode[1], ifDescr
linkDown	fcIfOperStatusCause[1], ifDescr

1. Added for Fibre Channel interfaces only. Refer to the CISCO-FC-FE-MIB.