



Multicast VPN MIB

First Published: August 9, 2004

Last Updated: August 21, 2007

The Multicast VPN MIB feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring of a Multicast VPN (MVPN) using the MVPN MIB (CISCO-MVPN-MIB).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Multicast VPN MIB”](#) section on page 7.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Prerequisites for Multicast VPN MIB

- Before performing the tasks in this module, you must configure MVPN. For information, see the [“Configuring Multicast-VPN”](#) chapter in the *Cisco IOS Multicast Configuration Guide*.
- You must configure SNMP on the routers on which the MVPN MIB is to be used. See the [“Configuring the Router to Send MVRP Trap Notifications”](#) task for more information. For more information about configuring an SNMP server, see the [“Configuring SNMP Support”](#) chapter in the *Cisco IOS Network Management Configuration Guide*.

Restrictions for Multicast VPN MIB

- Currently only IPv4 is supported.
- For all MIB objects with “read-create” access privileges, currently only “read-only” access is supported.



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

© 2004–2007 Cisco Systems, Inc. All rights reserved.

Information About Multicast VPN MIB

To configure the Multicast VPN MIB feature, you should understand the following concepts:

- [Overview of the MVPN MIB, page 2](#)
- [MVPN Information Retrieval Using SNMP and the MVPN MIB, page 2](#)
- [MVPN MIB Objects, page 2](#)

Overview of the MVPN MIB

In an MVPN network, a Provider Edge (PE) router has a multicast routing table and a Protocol Independent Multicast (PIM) instance associated with every VPN routing and forwarding (VRF) table that is used to define the VPN membership of customer sites attached to the router. There is one global multicast routing table and a table per multicast VRF (MVRF) used to route multicast packets received from a Customer Edge (CE) router. A set of MVRFs form a multicast domain (MD) when they are connected to potential sources and receivers of multicast traffic. A distinct group address, also known as the Multicast Distribution Tree (MDT) group address, obtained from an administrative pool, is assigned to each multicast domain. MDT groups are used by Provider Edge (PE) routers to encapsulate and transport multicast traffic within an MD through multicast tunnel interfaces (MTIs).

Initially all multicast data is forwarded using preconfigured MDT default groups. When certain multicast streams exceed a configured bandwidth threshold on the PE router, the multicast data is moved to an MDT data group that is dynamically chosen from an available pool of multicast addresses.

Using the MVPN MIB, network administrators can access MVRF information from PE routers for VPN traffic across multiple CE sites in real time. SNMP operations can be performed to monitor the MVRFs on the PE routers using **get** and **set** commands entered on the network management system (NMS) workstation for which SNMP has been implemented. The NMS workstations is also known as the SNMP manager.

MVPN Information Retrieval Using SNMP and the MVPN MIB

SNMP has historically been used to collect network information. SNMP permits retrieval of critical information from network elements such as routers, switches, and workstations. The MVPN MIB uses SNMP to configure MVRF trap notifications and to gather useful MVPN information in real time.

The MVPN MIB allows MVPN data for the managed devices on your system to be retrieved by SNMP. You can specify the retrieval of MVPN information from a managed device (for example, a router) either by entering commands on that managed device or by entering SNMP commands from the NMS workstation to gather MVPN information. MVPN MIB requests for information are sent from an NMS workstation to the router using SNMP and is retrieved from the router. This information can then be stored or viewed, thus allowing MVPN information to be easily accessed and transported across a multivendor programming environment.

MVPN MIB Objects

The MVPN MIB defines managed objects that enable a network administrator to remotely monitor the following MVPN information:

- The state of the MVRFs including the name of the MVRF, whether they are active, and the number of active multicast-enabled interfaces

- MDT default group address and encapsulation information
- Next hop information used to receive Border Gateway Protocol (BGP) MDT updates for Source Specific Multicast (SSM) mode
- Traffic threshold that determines switchover to an MDT data group
- Type of MDT group being used for a given (S, G) multicast route entry that exists on each configured MVRF, source address, and group address of the multicast route entry
- Source and group address used for encapsulation
- Information on MDT data groups currently joined
- Information on MVPN-specific MDT tunnels present in the device
- Trap notifications enabled on the router

**Note**

For a complete description of the objects supported by the MVPN MIB, see the CISCO_MVPN_MIB.my file, available on Cisco.com at <http://www.cisco.com/go/mibs>.

How to Configure Multicast VPN MIB

This section contains the following required procedure:

- [Configuring the Router to Send MVRF Trap Notifications, page 3](#) (required)

Configuring the Router to Send MVRF Trap Notifications

Perform this task to configure the router to use SNMP to send MVRF trap notifications.

MVRF Trap Notifications

An MVPN router can be configured to send MVRF (ciscoMvpnMvrfChange) trap notifications. A ciscoMvpnMvrfChange trap notification signifies a change about an MVRF in the device. The change event can be the creation of an MVRF, the deletion of an MVRF, or an update on the default or data multicast distribution tree (MDT) configuration of an MVRF. The change event is indicated by the ciscoMvpnGenOperStatusChange object embedded in the trap notification.

**Note**

Before the MVPN MIB can be used, the SNMP server for the router must be configured. To enable the SNMP server on the router, perform Steps 3 and 4. If an SNMP server is already available, omit Steps 3 and 4 and proceed to Step 5.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community *string* ro**
or
snmp-server community *string* rw

4. **snmp-server host** {*hostname* | *ip-address*} **version 2c** *community-string*
5. **snmp-server enable traps mvpn**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>snmp-server community <i>string</i> ro or snmp-server community <i>string</i> rw</p> <p>Example: Router(config)# snmp-server community public ro or Router(config)# snmp-server community public rw</p>	<p>Sets up the community access string to permit access to SNMP.</p> <ul style="list-style-type: none"> • The <i>string</i> argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • Specifying the snmp-server community command with the ro keyword configures read-only access. SNMP management stations using this string only can retrieve MIB objects. <p>or</p> <ul style="list-style-type: none"> • Specifying the snmp-server community command with the rw keyword configures read-write access. SNMP management stations using this string can retrieve and modify MIB objects.
Step 4	<p>snmp-server host {<i>hostname</i> <i>ip-address</i>} version 2c <i>community-string</i></p> <p>Example: Router(config)# snmp-server host 192.168.1.1 version 2c public</p>	<p>Specifies the recipient of an SNMP notification operation.</p>
Step 5	<p>snmp-server enable traps mvpn</p> <p>Example: Router(config)# snmp-server enable traps mvpn</p>	<p>Enables the router to send MVRFP trap notifications.</p>
Step 6	<p>end</p> <p>Example: Router(config)# end</p>	<p>Exits the current configuration mode and returns to privileged EXEC mode.</p>

Configuration Examples for Multicast VPN MIB

This section provides the following configuration example:

- [Configuring the Router to Send MVRF Trap Notifications: Example, page 5](#)

Configuring the Router to Send MVRF Trap Notifications: Example

The following example shows how to configure a router to use SNMP to send MVRF trap notifications:

```
!  
snmp-server community public RW  
snmp-server enable traps mvpn  
snmp-server host 10.3.32.154 version 2c public  
!
```

Additional References

The following sections provide references related to the Multicast VPN MIB feature.

Related Documents

Related Topic	Document Title
MVPN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS IP Multicast Command Reference
SNMP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Network Management Command Reference

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> CISCO-MVPN-MIB.my 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

RFCs

RFC	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS IP Multicast Command Reference* at http://www.cisco.com/en/US/docs/ios/ipmulti/command/reference/imc_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- snmp-server enable traps mvpn**

Feature Information for Multicast VPN MIB

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Multicast VPN MIB

Feature Name	Releases	Feature Information
Multicast VPN MIB	12.0(29)S 12.3(14)T 12.2(33)SRA 12.2(33)SXH	The Multicast VPN MIB feature introduces the capability for SNMP monitoring of an MVPN using the MVPN MIB (CISCO-MVPN-MIB). The following command was introduced by this feature: snmp server enable traps mvpn

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2004–2007 Cisco Systems, Inc. All rights reserved.

