Multicast VPN MIB

Last Updated: August 29, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to 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.
- You must configure SNMP on the routers on which the MVPN MIB is to be used.

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.

Information About Multicast VPN MIB

Overview of the MVPN MIB

In an MVPN network, a provider pdge (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 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 are 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 .

- MVRF Trap Notifications, page 3

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.

How to Configure Multicast VPN MIB

- Configuring the Router to Send MVRF Trap Notifications, page 3

Configuring the Router to Send MVRF Trap Notifications

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

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. Do one of the following:
   - **snmp-server community** *string* **ro**
   -
   - **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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **snmp-server community** *string* **ro**
	•
	• **snmp-server community** *string* **rw**
	
	Example:
	`Router(config)# snmp-server community public ro`
	
	Example:
	
	Example:
	`Router(config)# snmp-server community public rw`
		Sets up the community access string to permit access to SNMP.
		• The *string* 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 can only retrieve MIB objects.
		or
		• 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.

	Command or Action	Purpose
Step 4	**snmp-server host {** *hostname* **|** *ip* **-** *address* **} version 2c** *community* **-** *string* **Example:** `Router(config)# snmp-server host 192.168.1.1 version 2c public`	Specifies the recipient of an SNMP notification operation.
Step 5	**snmp-server enable traps mvpn** **Example:** `Router(config)# snmp-server enable traps mvpn`	Enables the router to send MVRF trap notifications.
Step 6	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuration Examples for Multicast VPN MIB

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

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
• CISCO-MVPN-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Multicast VPN MIB

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

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**

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.