PIM MIB Extension for IP Multicast

Feature History

Release	Modification
12.0(15)S	This feature was introduced.
12.2(4)T	This feature was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.

This document describes the PIM MIB Extension for IP Multicast feature in Cisco IOS Release 12.2(14)S. It includes the following sections:

Feature Overview

Protocol Independent Multicast (PIM) is an IP Multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the *Protocol Independent Multicast for IPv4* MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

The PIM MIB Extension for IP Multicast feature introduces support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the existing Cisco implementation of the PIM MIB. This feature introduces the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - When a router's PIM interface is disabled or enabled (using the **ip pim** command in interface configuration mode)
  - When a router's PIM neighbor adjacency expires or is established (defined in RFC 2934)
- rp-mapping-change—This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.

- invalid-pim-message—This notification results from the following conditions:
  - When an invalid (*, G) join or prune message is received by the device (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group)
  - When an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

Benefits

- Allows users to identify changes in the multicast topology of their network by detecting changes in the RP mapping.
- Provides traps to monitor the PIM protocol on PIM-enabled interfaces.
- Helps users identify routing issues when multicast neighbor adjacencies expire or are established on a multicast interface.
- Enables users to monitor RP configuration errors (for example, errors due to flapping in dynamic RP allocation protocols like Auto-RP).

Restrictions

The following MIB tables are not supported in Cisco IOS software:

- pimIpMRouteTable
- pimIpMRouteNextHopTable

The pimInterfaceVersion object was removed from RFC 2934 and, therefore, is no longer supported in Cisco IOS software.

Related Documents

For information on configuring IP multicast using Cisco IOS software, refer to the following documents:

- *Cisco IOS IP Configuration Guide*, Release 12.2.
- *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.2

For information on configuring SNMP using Cisco IOS software, refer to the following documents:

- "Configuring SNMP Support" chapter, *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.2
- "SNMP Commands" chapter, *Cisco IOS Configuration Fundamentals Command Reference*, Release 12.2.

Supported Platforms

This feature is supported on all platforms that support the PIM-MIB and Cisco IOS Release 12.2(14)S, Release 12.2(4)T, Release 12.0(15)S, or later releases.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

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

http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

This feature introduces support in Cisco IOS software for the CISCO-PIM-MIB. The MIB file CISCO-PIM-MIB.my can be downloaded from the Cisco MIB website on Cisco.com at the following URL:

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

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download other MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

RFCs

The CISCO-PIM-MIB partially supports RFC 2934. For more information, see the "Restrictions" section on page 2.

Configuration Tasks

See the following sections for configuration tasks for the PIM MIB Extension for IP Multicast feature. Each task in the list is identified as either required or optional:

- Configuring Cisco PIM SNMP Traps (required)
- Verifying the Cisco PIM MIB (optional)

Configuring Cisco PIM SNMP Traps

To configure a router to send PIM trap notifications to a specified host, use the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# snmp-server enable traps pim [neighbor-change | rp-mapping-change | invalid-pim-message]`	Enables a router to send PIM notifications. The keywords are as follows: • **neighbor-change**—Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires or is established. • **rp-mapping-change**—Enables notifications indicating a change in RP mapping information due to either Auto-RP or BSR messages. • **invalid-pim-message**—Enables notifications for monitoring invalid PIM protocol operations (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group or when a router receives a register message from a multicast group for which it is not the RP).
Step 2	`Router(config)# snmp-server host host-addr [traps | informs] community-string pim`	Specifies the recipient of a PIM SNMP notification operation.

Verifying the Cisco PIM MIB

To verify the configuration of PIM notifications, use the **show running-config** command.

Configuration Examples

This example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
router(config)# snmp-server host 10.0.0.1 traps version 2c public pim
```

```
! Configure router to send the neighbor-change class of notifications to host.
router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
router(config)# interface ethernet0/0
router(config-if)# ip pim sparse-dense-mode
```

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- **snmp-server enable traps pim**
- **snmp-server host**

snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim** command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps pim [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires or is established.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables notifications for monitoring invalid PIM protocol operations (for example, when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group or when a router receives a register message from a multicast group for which it is not the RP).

Defaults

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files available from the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
router(config)# snmp-server enable traps pim neighbor-change
```

```
! Enable PIM sparse-dense mode on Ethernet interface 0/0.
router(config)# interface ethernet0/0
router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

snmp-server host *host-addr* [**traps | informs**] [**version** {**1 | 2c | 3** [**auth | noauth | priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host *host-addr* [**traps | informs**]

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Sends SNMP traps to this host. This is the default.
informs	(Optional) Sends SNMP informs to this host.
version	(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C. • **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword: – **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth	noauth	priv**] keyword choice is not specified. – **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called "privacy").
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.
udp-port *port*	(Optional) UDP port of the host to use. The default is 162.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: • **bgp**—Sends Border Gateway Protocol (BGP) state change notifications. • **calltracker**—Sends Call Tracker call-start/call-end notifications. • **config**—Sends configuration notifications. • **dspu**—Sends downstream physical unit (DSPU) notifications. • **entity**—Sends Entity MIB modification notifications. • **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. • **frame-relay**—Sends Frame Relay notifications. • **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. • **isdn**—Sends Integrated Services Digital Network (ISDN) notifications. • **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications. • **pim**—Sends Protocol Independent Multicast (PIM) notifications. • **repeater**—Sends standard repeater (hub) notifications. • **rsrb**—Sends remote source-route bridging (RSRB) notifications. • **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications. • **rtr**—Sends SA Agent (RTR) notifications. • **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications. • **sdllc**—Sends SDLLC notifications. • **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications. • **stun**—Sends serial tunnel (STUN) notifications. • **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. • **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command. • **x25**—Sends X.25 event notifications.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. In order to disable informs, use the **no snmp-server host informs** command.

Note If the *community-string* argument is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This is the default behavior for Cisco IOS Release 12.0(3) and later releases.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The following keywords were added: • **version 3** [**auth** | **noauth** | **priv**] • **hsrp**
11.3(1) MA, 12.0(3)T	The **voice** notification-type keyword was added.
12.1(3)T	The **calltracker** notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(4)T	The **pim** notification-type keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification-type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command help **?** at the end of the **snmp-server host** command.

Examples

If you want to configure a unique snmp community string for traps, but you want to prevent snmp polling access with this string, the configuration should include an access-list. In the following example, the community string is named "comaccess" and the access list is numbered 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```

The following example sends RFC 1157 SNMP traps to the host specified by the name myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
Router(config)# snmp-server enable traps snmp
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host bob public isdn
```

The following example enables the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP notifications (traps and informs).
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Defines how often to try resending trap messages on the retransmission queue.

Glossary

inform—An SNMP trap message that includes a delivery confirmation request.

Management Information Base—See MIB.

MIB—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP) or Common Management Information Protocol (MIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

PIM—An IP multicast routing protocol used for routing multicast data packets to multicast groups. PIM is unicast routing protocol-independent and can operate in different modes such as sparse mode and dense mode.

Protocol Independent Multicast—See PIM.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. An application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap—Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.