



HSRP MIB

This feature module describes the addition of HSRP MIB support for Simple Network Management Protocol (SNMP) in Cisco IOS Release 12.0(12)S. It includes information on the benefits of the new feature, supported platforms, supported standards, and the modified Cisco IOS commands used to enable HSRP monitoring.

This document includes the following sections:

- Feature Overview, page 1
- Supported Platforms, page 2
- Supported Standards, MIBs, and RFCs, page 2
- Configuration Tasks, page 3
- Configuration Examples, page 4
- Command Reference, page 4
- Glossary, page 13

Feature Overview

Hot Standby Router Protocol (HSRP) is a protocol developed by Cisco which provides high network availability and transparent network topology changes. Cisco IOS Release 12.0(12)S adds support for the HSRP MIB (previously supported in Cisco IOS 12.0 T releases and Cisco IOS 12.1-based releases only), which allows the monitoring and configuration of HSRP groups using Simple Network Management Protocol (SNMP).

SNMP Get operations can be used from a network management system (NMS) to get reports about HSRP groups in a network. HSRP MIB support also allows you to enable or disable the sending of SNMP notifications from the Cisco IOS command-line interface (CLI). These notifications (traps or informs) are sent to the NMS when a routing device leaves or enters the active or standby state.

Four MIB tables are supported by this feature: cHsrpGrpEntry table, defined in CISCO-HSRP-MIB.my, and cHsrpExtIfTrackedEntry, cHsrpExtSecAddrEntry, and cHsrpExtIfEntry, defined in CISCO-HSRP-EXT-MIB.my. The cHsrpGrpEntry table consists of all the group information defined in RFC 2281, *Cisco Hot Standby Router Protocol*; the other tables consist of the Cisco extensions to RFC 2281, which are defined in CISCO-HSRP-EXT-MIB.my

Benefits

Allows the monitoring of HSRP activity through network management applications.

Restrictions

The Cisco IOS software supports a read-only version of the MIB, and Set operations are not supported.

Related Features and Technologies

- Hot Standby Router Protocol (HSRP)
- Simple Network Management Protocol (SNMP)

Related Documents

For information about HSRP, see the chapter “Using HSRP for Fault-Tolerant IP Routing” in the *Internetworking Case Studies* document.

For information about SNMP, see the chapter “Monitoring the Router and Network” in the *Configuration Fundamentals Configuration Guide*, Release 12.0.

Supported Platforms

The HSRP MIB is supported on all Cisco platforms which support both HSRP and SNMP. Cisco IOS Release 12.0(12)S adds support for the HSRP MIB on the following platforms:

- Cisco 7200 series
- Cisco 7500/RSP series
- Cisco 12000 GSR series

Supported Standards, MIBs, and RFCs

Standards

No standards are supported for this feature.

MIBs

HSRP MIB support consists of the following MIBs and related files:

- CISCO-HSRP-CAPABILITY.my
- CISCO-HSRP-EXT-CAPABILITY.my
- CISCO-HSRP-EXT-MIB.my
- CISCO-HSRP-MIB.my

For lists of supported MIBs by platform, and to download Cisco MIBs, go to the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

RFCs

RFC 2281, *Cisco Hot Standby Router Protocol*

Configuration Tasks

Perform the following tasks to enable HSRP trap support and verify HSRP trap operation.

- Enabling HSRP Traps
- Verifying HSRP Operation

Enabling HSRP Traps

HSRP MIB trap support is enabled using the **hsrp** option in the **snmp-server enable** and **snmp-server host** commands, as follows.

	Command	Purpose
Step 1	Router(config)# snmp-server enable traps hsrp	Enables the router to send HSRP notifications using SNMP.
Step 2	Router(config)# snmp-server host <i>host-address</i> <i>community-string</i> hsrp	Specifies the recipient of an SNMP notification operation, and that HSRP notifications will be sent to the specified host. See the command reference section of this document for a list of all optional keywords and arguments.

Verifying HSRP Operation

Use the following procedure to verify that the HSRP feature is enabled:

For each network that has had HSRP configured, enter the **show standby** command to verify the protocol is running.

```
Router# show standby

Ethernet0 - Group 0
  Local state is Active, priority 100, may preempt
  Hello time 3 hold time 10
  Next hello sent in 0:00:00
  Hot standby IP address is 198.92.72.29 configured
  Active router is local
  Standby router is 198.92.72.21 expires in 0:00:07
  Standby virtual mac address is 0000.0c07.ac00
  Tracking interface states for 2 interfaces, 2 up:
    Up    Serial0
    Up    Serial1
```

The local state report indicates the state of the router, and can be one of the following:

- Active—Current Hot Standby router.

- Standby—Router next in line to be the Hot Standby router.
- Speak—Router is sending packets to claim the active or standby role.
- Listen—Router is neither active nor standby, but if no messages are received from the active or standby router, it will start to speak.
- Learn—Router is neither active nor standby, nor does it have enough information to attempt to claim the active or standby roles.
- Init—Router is not yet ready to participate in HSRP, possibly because the associated interface is not up.

Configuration Examples

The following examples show how to configure HSRP on two routers and enable the HSRP MIB trap support feature. As in many environments, one router is preferred as the active one. This is realized by configuring it at a higher priority level and enabling preemption. In the following example, the active router is referred to as the primary router. The second router is referred to as the backup router:

Primary Router

```
interface Ethernet1
 ip address 15.1.1.1 255.255.0.0
 no ip redirects
 standby priority 200 preempt
 standby preempt
 standby ip 15.1.1.3
 snmp-server enable traps hsrp
 snmp-server host yourhost.cisco.com public hsrp
```

Backup Router

```
interface Ethernet1
 ip address 15.1.1.2 255.255.0.0
 no ip redirects
 standby priority 101
 standby ip 15.1.1.3
 snmp-server enable traps hsrp
 snmp-server host myhost.cisco.com public hsrp
```

Command Reference

This section documents the following modified commands for the HSRP MIB feature. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

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

snmp-server enable traps

To enable the router to send SNMP traps and informs, use the **snmp-server enable traps** global configuration command. To disable SNMP notifications, use the **no** form of this command.

snmp-server enable traps [*notification-type*] [*notification-option*]

no snmp-server enable traps [*notification-type*] [*notification-option*]

Syntax Description	
<i>notification-type</i>	<p>(Optional) Type of notification to enable or disable. If no type is specified, all notifications supported on your routing device are enabled or disabled. Not all notification types are available for all Cisco platforms. The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"> • bgp—Controls (enables or disables) Border Gateway Protocol (BGP) state change notifications. • config—Controls configuration notifications. • entity—Controls Entity MIB modification notifications. • envmon—Controls Cisco enterprise-specific environmental monitor notifications. Notifications are sent when an environmental threshold is exceeded. When the envmon keyword is used, you can specify a <i>notification-option</i> value. • frame-relay—Controls Frame Relay notifications. • hsrp—Controls Hot Standby Routing Protocol (HSRP) notifications. • isdn—Controls Integrated Services Digital Network (ISDN) notifications. When the isdn keyword is used on Cisco 1600 series routers, you can specify a <i>notification-option</i> value. • msdp—Controls Multicast Source Discovery Protocol (MSDP) notifications. • repeater—Controls Ethernet hub repeater notifications. When the repeater keyword is selected, you can specify a <i>notification-option</i> value. • rtr—Controls response time reporter (RTR) notifications. • snmp—Controls Simple Network Management Protocol (SNMP) notifications (defined in RFC 1157). The following notification types are controlled by the snmp-server enable traps snmp command: authentication, linkup, linkdown, coldstart, and warmstart. You can use the authentication keyword to specifically enable or disable authentication notifications (see below). • syslog—Controls Cisco Syslog MIB error message notifications. Specify the level of messages to be sent with the logging history level command.

notification-option

- **envmon [voltage | shutdown | supply | fan | temperature]**
When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**.
- **isdn [call-information | isdn u-interface]**
When the **isdn** keyword is used, you can specify the call-information keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdn u-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem.
- **repeater [health | reset]**
When the **repeater** keyword is used, you can specify the **repeater** option. If no option is specified, all repeater notifications are enabled. The option can be either of the following keywords:
 - **health**—Enables Repeater Hub MIB health notification.
 - **reset**—Enables Repeater Hub MIB reset notification.
- **snmp [authentication]**
When the **snmp** keyword is used, you can specify the **authentication** option to specifically enable or disable SNMP Authentication Failure notifications. (The **snmp-server enable traps snmp authentication** command replaces the **snmp-server trap-authentication** command.) If no option is specified, all SNMP notifications are enabled. For definitions of SNMP notification types, see RFC 1157.

Defaults

This command is disabled by default. Most notification types are disabled. However, some notification types cannot be controlled with this command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, linkUp/linkDown notifications for specific interfaces are controlled by the **snmp trap link-status** command.

If you enter this command with no *notification-type* keywords, the default is to enable all notification types controlled by this command.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(12)S	The following keywords were added for the 12.0 S train: <ul style="list-style-type: none"> • hsrp • msdp

Usage Guidelines

This command is useful for disabling notifications that are generating a large amount of useless noise. SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. To configure the router to send these SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, you must issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, you must configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, just the appropriate **snmp-server host** command must be enabled.

The notification types used in this command all have an associated MIB object that allows them to be globally enabled or disabled. Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these notifications cannot be controlled using the **snmp-server enable traps** command.

Examples

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

```
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

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

```
snmp-server enable traps
snmp-server host myhost.cisco.com public
```

The following example enables the router to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
snmp-server enable traps frame-relay
snmp-server enable traps envmon temperature
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 the only the ISDN traps enabled to be sent to a host.

```
snmp-server enable traps bgp
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:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands	Command	Description
	snmp-server host	Specifies the recipient of an SNMP notification operation.
	snmp-server informs	Specifies inform request options.
	snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server host

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. To remove the specified host from the configuration, use the **no** form of this command.

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

```
no snmp-server host host [traps | informs] [notification-type]
```

Syntax Description	
<i>host</i>	Name or Internet address of the host.
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. <ul style="list-style-type: none"> • 1—SNMPv1. This option is the default, and is not available with informs. • 2c—SNMPv2c (also referred to as SNMPv2p). • 3—SNMPv3 <ul style="list-style-type: none"> – auth—(Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. – priv—(Optional) Enables Data Encryption Standard (DES) packet encryption (also called privacy). – noauth—(Optional) Specifies that no authentication checking is necessary. <p>Note: If you specify SNMPv3 without the auth or priv keywords, the noAuthNoPriv security level is assumed.</p>
<i>community-string</i>	Password-like community string sent with the notification operation.
udp-port <i>port</i>	(Optional) UDP port of the host to use. The default is 162.

<i>notification-type</i>	<p>(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:</p> <ul style="list-style-type: none"> • bgp—Controls Border Gateway Protocol (BGP) state change notifications. • config—Controls configuration notifications. • dspu—Controls downstream physical unit (DSPU) notifications. • entity—Controls Entity MIB modification notifications. • envmon—Controls Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the envmon keyword is used, you can specify a <i>notification-option</i> value. • frame-relay—Controls Frame Relay notifications. • hsrp—Controls Hot Standby Routing Protocol (HSRP) notifications. • isdn—Controls Integrated Services Digital Network (ISDN) notifications. • llc2—Controls Logical Link Control, type 2 (LLC2) notifications. • msdp—Controls Multicast Source Discovery Protocol (MSDP) notifications. • rptr—Controls standard repeater (hub) notifications. • rsrb—Controls remote source-route bridging (RSRB) notifications. • rtr—Controls Service Assurance Agent response time reporter (RTR) notifications. • sdlc—Controls Synchronous Data Link Control (SDLC) notifications. • sdllc—Controls SDLC Logical Link Control (SDLLC) notifications. • snmp—Controls Simple Network Management Protocol (SNMP) notifications (defined in RFC 1157). • stun—Controls serial tunnel (STUN) notifications. • syslog—Controls error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the logging history level command. • tty—Controls Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • x25—Controls 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. If no **traps** or **informs** keyword is present, traps are enabled.

The **no snmp-server host** command with no keywords will disable traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.1(3)T	The hsrp keyword was added for the Cisco IOS Release 12.1 T train.
	12.0(12)S	The hsrp keyword was added for the Cisco IOS Release 12.0 S train.

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 controlled by this command are sent. To configure the router to send those 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. 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.

However, some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

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 (for example, the Cisco 12000 series GSR platforms use the environmental monitor).

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

```
snmp-server enable traps hsrp
snmp-server host myhost.cisco.com traps version 2c public hsrp
```

The following example sends the SNMP traps defined in RFC 1157 to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

```
snmp-server enable traps
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:

```
snmp-server enable traps
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:

```
snmp-server enable traps
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.

```
snmp-server enable traps bgp
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:

```
snmp-server enable traps
snmp-server host myhost.cisco.com informs version 2c public
```

Related Commands

Command	Description
snmp-server enable traps	Enables the sending of SNMP traps and informs.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) that an SNMP trap should originate from.
snmp-server trap-timeout	Defines how often the system should try resending trap messages.

Glossary

Hot Standby Routing Protocol—See HSRP.

HSRP—Hot Standby Routing Protocol. Protocol used among a group of routers for selecting an active router and a standby router. (An active router is the router of choice for routing packets; a standby router is a router that takes over the routing duties when an active router fails, or when preset conditions are met.)

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 SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

Simple Network Management Protocol—See SNMP.

SNMP—Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

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

