snmp-server enable traps ospf cisco-specific state-change

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) transition state changes, use the **snmp-server enable traps ospf cisco-specific state-change** command in global configuration mode. To disable OSPF transition state change SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

no snmp-server enable traps ospf cisco-specific state-change [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]

Syntax Description

nssa-trans-change	(Optional) Enables only not-so-stubby area (NSSA) translator state changes trap for the OSPF area.
shamlink	(Optional) Enables only the sham-link transition state changes trap for the OSPF area.
interface	(Optional) Enables only the sham-link interface state changes trap for the OSPF area.
interface-old	(Optional) Enables only the replaced interface transition state changes trap for the OSPF area.
neighbor	(Optional) Enables only the sham-link neighbor transition state changes trap for the OSPF area.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF transition state changes are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.0(30)S	The **shamlink**, **interface-old**, and **neighbor** keywords were added.
12.3(14)T	Support was added for the **shamlink**, **interface-old**, and **neighbor** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.

Examples

The following example enables the router to send OSPF sham-link transition state change notifications to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.

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 the PIM interface on a router is disabled or enabled, or when the PIM neighbor adjacency on a router 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 invalid PIM message traps. For example, an invalid PIM message could result 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.

Command Default

SNMP notifications are disabled.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 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 on 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 enable traps pppoe

To enable Point-to-Point Protocol over Ethernet (PPPoE) session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe** command in global configuration mode. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

snmp-server enable traps pppoe

no snmp-server enable traps pppoe

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DC	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session-count thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of this notification and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/public/mibs/v2/.

Examples

The following example enables the router to send PPPoE session-count SNMP notifications to the host at the address 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

Related Commands

Command	Description
pppoe limit max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.
pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

Command	Description
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 enable traps repeater

To enable or disable standard repeater (hub) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps repeater** command in global configuration mode. To disable repeater notifications, use the **no** form of this command.

snmp-server enable traps repeater [**health**] [**reset**]

no snmp-server enable traps repeater [**health**] [**reset**]

Syntax Description

health	(Optional) Enables the rptrHealth trap, which conveys information related to the operational status of the repeater.
reset	(Optional) Sends the rptrResetEvent trap on completion of a repeater reset action (triggered by the transition to a START state by a manual command).

Command Default

SNMP notifications are disabled.

If no option keywords are specified when entering this command, all repeater notifications available on your system are enabled or disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command enables or disables Repeater MIB notifications, as defined in RFC 1516. RFC 1516 defines objects for managing IEEE 802.3 10 Mbps baseband repeaters, also known as hubs.

Two sets of notifications are available for this command. The following notification is defined in the CISCO-REPEATER-MIB (enterprise 1.3.6.1.4.1.9.9.22.3):

- 1 ciscoRptrIllegalSrcAddrTrap (illegal source address trap)

The following notifications are defined in the CISCO-REPEATER-MIB-V1SMI (enterprise 1.3.6.1.2.1.22):

- 1 rptrHealth
- 2 rptrGroupChange
- 3 rptrResetEvent

For a complete description of the repeater notifications and additional MIB functions, refer to the CISCO-REPEATER-MIB.my and CISCO-REPEATER-MIB-V1SMI.my files, available on Cisco.com at

http://www.cisco.com/public/mibs/.

When the optional **health** keyword is used, the rptrHealth trap is sent when the value of rptrOperStatus changes, or upon completion of a nondisruptive test.

The rptrOperStatus object indicates the operational state of the repeater. Status values are as follows:

- other(1)—undefined or unknown status
- ok(2)—no known failures
- rptrFailure(3)—repeater-related failure
- groupFailure(4)—group-related failure
- portFailure(5)—port-related failure
- generalFailure(6)—failure, unspecified type

When the optional **reset** keyword is used, the rptrResetEvent trap is not sent when the agent restarts and sends an SNMP coldStart or warmStart trap.

The **snmp-server enable traps repeater** 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 SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send repeater inform notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps repeater
Router(config)# 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 trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps resource-policy

To enable Embedded Resource Manager (ERM)-MIB notification traps, use the **snmp-server enable traps resource-policy** command in global configuration mode. To disable the ERM-MIB notification traps, use the **no** form of this command.

snmp-server enable traps resource-policy

no snmp-server enable traps resource-policy

Syntax Description

This command has no arguments or keywords.

Command Default

Notification traps will be sent to the host that is configured to receive traps.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Examples

The following example shows how to configure the router to send SNMP notifications for ERM to a host:

```
Router(config)# snmp-server enable traps resource policy
```

Related Commands

Command	Description
snmp-server community	Permits access to SNMP by setting up the community access string.
snmp-server host	Specifies the recipient of an SNMP notification message.

snmp-server enable traps rtr

To enable the sending of Cisco IOS IP Service Level Agreements (SLAs) Simple Network Management Protocol (SNMP) trap notifications, use the **snmp-server enable traps rtr** command in global configuration mode. To disable IP SLAs SNMP notifications, use the **no** form of this command.

snmp-server enable traps rtr

no snmp-server enable traps rtr

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command controls (enables or disables) Cisco IOS IP SLAs notifications, as defined in the Response Time Monitor MIB (CISCO-RTTMON-MIB).

The **snmp-server enable traps rtr** 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 SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send IP SLAs SNMP traps to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.

Command	Description
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps snmp

To enable the RFC 1157 Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps snmp** command in global configuration mode. To disable RFC 1157 SNMP notifications, use the **no** form of this command.

snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

no snmp-server enable traps snmp [**authentication**] [**linkup**] [**linkdown**] [**coldstart**] [**warmstart**]

Syntax Description

authentication	(Optional) Controls the sending of SNMP authentication failure notifications.
linkup	(Optional) Controls the sending of SNMP linkUp notifications.
linkdown	(Optional) Controls the sending of SNMP linkDown notifications.
coldstart	(Optional) Controls the sending of SNMP coldStart notifications.
warmstart	(Optional) Controls the sending of SNMP warmStart notifications.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	The **snmp-server enable traps snmp authentication** command was introduced. This command replaced the **snmp-server trap-authentication** command.
12.1(3)T	The following keywords were added: • **linkup** • **linkdown** • **coldstart**
12.1(5)T	The **warmstart** keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

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.

If you do not enter an **snmp-server enable traps snmp** 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 snmp** command. When you enter the command with no keywords, all notification types are enabled. When you enter the command with a keyword, only the types of notifications related to that keyword are enabled.

When you use the optional **authentication** keyword, the authenticationFailure(4) trap signifies that the sending device is the addressee of a protocol message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs for packets with an incorrect community string and the SNMP traps are generated. For SNMPv3, authentication failure occurs for packets with an incorrect SHA/MD5 authentication key or for a packet that is outside the authoritative SNMP engine's window (for example, packets that are configured outside access lists or time ranges) and a report PDU is generated, however authentication failure traps are not generated.

When you use the optional **linkup** keyword, the linkUp(3) trap signifies that the sending device recognizes one of the communication links represented in the agent's configuration coming up.

When you use the optional **linkdown** keyword, the linkDown(2) trap signifies that the sending device recognizes a failure in one of the communication links represented in the agent's configuration.

The **snmp-server enable traps snmp** [**linkup**] [**linkdown**] form of this command globally enables or disables SNMP linkUp and linkDown traps. After enabling either of these traps globally, you can disable them on specific interfaces using the **no snmp trap link-status** command in interface configuration mode. On the interface level, linkUp and linkDown traps are enabled by default, which means that these notifications do not have to be enabled on a per-interface basis. However, linkUp and linkDown notifications will not be sent unless you enable them globally using the **snmp-server enable traps snmp** command.

When you use the optional **coldstart** keyword, the coldStart(0) trap signifies that the sending device is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

When you use the optional **warmstart** keyword, the warmStart(1) trap signifies that the sending device is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.

The **snmp-server enable traps snmp** 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. In order to send notifications, you must configure at least one **snmp-server host** command.

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

Examples

The following example shows how to enable the router to send all traps to the host myhost.cisco.com, using the community string public:

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

The following example shows how to enable the router to send all inform notifications to the host myhost.cisco.com using the community string public:

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

The following example shows how to enable all SNMP trap types, and then disable only the linkUp and linkDown traps:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps snmp
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart

Router# configure terminal
Router(config)# no snmp-server enable traps snmp linkup linkdown
Router(config)# end
Router# more system:running-config | include traps snmp
snmp-server enable traps snmp authentication coldstart warmstart
```

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 informs	Specifies inform request options.
snmp-server trap authentication vrf	Disables or reenables SNMP authentication notifications specific to VPN context mismatches.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps srp

To enable the sending of Intelligent Protection Switching (IPS) Spatial Reuse Protocol (SRP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps srp** command in global configuration mode. To disable SRP notifications, use the **no** form of this command.

snmp-server enable traps srp

no snmp-server enable traps srp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced to support DPT-OC12 Port Adapters.

Usage Guidelines

The Cisco SRP MIB module (CISCO-SRP-MIB.my) provides objects for monitoring IP-over-SONET IPS SRP traffic using the SNMP. When IPS is enabled, if a node or fiber facility failure is detected, traffic going toward or coming from the failure direction is wrapped (looped) back to go in opposite direction on the other ring.

The **snmp-server enable traps srp** command enables SRP state change notifications (traps or informs). SRP state change notifications are generated whenever one of the two sides of an SRP interface ring enters or leaves the wrapped state (when a ring wraps, or when a ring is restored).

Specifically, the srpMACIpsWrapCounter object in the CISCO-SRP-MIB increments when a Ring wraps, and the value of the rpMACIpsLastUnWrapTimeStamp object changes when a ring unwraps. (An "unwrap" event happens when the original ring is restored.)

The **snmp-server enable traps srp** 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 SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, SRP-specific informs are enabled and will be sent to the host "myhost.cisco.com" using the community string defined as public:

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

snmp-server enable traps storm-control

To enable Simple Network Management Protocol (SNMP) storm-control trap notifications, use the **snmp-server enable traps storm-control** command in privileged EXEC mode. To disable storm-control trap notifications, use the **no** form of this command.

snmp-server enable traps storm-control {**traps-rate** *num*}

no snmp-server enable traps storm-control {**traps-rate** *num*}

Syntax Description

traps-rate *num*	Number of traps per minute; valid values are 0 through 1000.

Command Default

Storm-control traps are disabled.

Command Modes

Configuration mode (config)

Command History

Release	Modification
12.2(33)SXJ	This command was introduced.

Examples

This example shows how to enable the storm-control trap notification trap rate to 250:

```
Router# snmp-server enable traps storm control traps-rate 250
Router#
```

Related Commands

Command	Description
snmp-server enable traps storm-control	Enables SNMP storm-control trap notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
test snmp trap storm-control	Tests the SNMP CISCO-PORT-STORM-CONTROL-MIB traps.

snmp-server enable traps syslog

To enable the sending of system logging message Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps syslog** command in global configuration mode. To disable system logging message SNMP notifications, use the **no** form of this command.

snmp-server enable traps syslog

no snmp-server enable traps syslog

Syntax Description

This command has no arguments or keywords.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) system logging message notifications. System logging messages (also called system error messages, or syslog messages) are status notification messages that are generated by the routing device during operation. These messages are typically logged to a destination (such as the terminal screen, to a system buffer, or to a remote “syslog” host).

If your software image supports the Cisco Syslog MIB, these messages can also be sent via SNMP to a network management station (NMS). To determine which software images support the Cisco Syslog MIB, used the Cisco MIB Locator tool at http://www.cisco.com/go/mibs/ .(At the time of writing, the Cisco Syslog MIB is only supported in “Enterprise” images.)

Unlike other logging processes on the system, debug messages (enabled using CLI debug commands) are not included with the logging messages sent via SNMP.

To specify the severity level at which notifications should be generated, use the **logging history** global configuration command. For additional information about the system logging process and severity levels, see the description of the **logging** commands.

The syslog notification is defined by the clogMessageGenerated NOTIFICATION-TYPE object in the Cisco Syslog MIB (CISCO-SYSLOG-MIB.my). When a syslog message is generated by the device a clogMessageGenerated notification is sent to the designated NMS. The clogMessageGenerated notification includes the following objects: clogHistFacility, clogHistSeverity, clogHistMsgName, clogHistMsgText, clogHistTimestamp.

For a complete description of these objects and additional MIB information, see the text of CISCO-SYSLOG-MIB.my, available on Cisco.com using the SNMP Object Navigator tool at http://www.cisco.com/go/mibs . See also the CISCO-SYSLOG-EXT-MIB and the CISCO-SYSLOG-EVENT-EXT-MIB.

The **snmp-server enable traps syslog** 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 SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example enables the router to send system logging messages at severity levels 0 (emergencies) through 2 (critical) to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
logging history	Limits syslog messages sent to the router's history table and to an SNMP NMS based on severity.
snmp-server host	Specifies the destination NMS and transfer parameters for SNMP notifications.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps transceiver

To enable all supported SNMP transceiver traps for all transceiver types in the global configuration mode, use the **snmp-server enable traps transceiver** command. Use the **no** form of this command to disable the transceiver SNMP trap notifications.

snmp-server enable traps transceiver type all

no snmp-server enable traps transceiver type all

Syntax Description

The command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **snmp-server enable traps** command is used 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.

Examples

This example shows how to enable all supported SNMP transceiver traps for all transceiver types:

```
Router(config)# snmp-server enable traps transceiver type all
Router(config)#
```

Related Commands

Command	Description
show interfaces transceiver	Displays information about the optical transceivers that have DOM enabled.

snmp-server enable traps voice

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

snmp-server enable traps voice [**poor-qov**] [**fallback**]

no snmp-server enable traps voice

Syntax Description

poor-qov	(Optional) Enables poor-quality-of-voice SNMP notifications.
fallback	(Optional) Enables SNMP fallback voice notifications.

Command Default

If you enter this command without any of the optional keywords, both available notifications are enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.3(14)T	The **fallback** keyword was added.

Usage Guidelines

SNMP notifications can be sent as traps (notifications) or inform requests. This command enables both traps and inform requests.

The **poor-qov** keyword enables or disables poor-quality-of-voice notifications. The poor quality-of-voice notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

enterprise 1.3.6.1.4.1.9.9.63.2

(1) cvdcPoorQoVNotification

The **fallback** keyword enables or disables public switched telephone network (PSTN) fallback notifications. The fallback notification is defined in CISCO-VOICE-DIAL-CONTROL-MIB as follows:

(1) cvVoIPCallHistoryConnectionId

(2) cvVoIPCallHistoryFallbackIcpif

(2) cvVoIPCallHistoryFallbackLoss

(3) cvVoIPCallHistoryFallbackDelay

(4) cvVoIPCallHistoryRemSigIPAddrT

(5) cvVoIPCallHistoryRemSigIPAddr

(6) cvVoIPCallHistoryRemMediaIPAddrT

(7) cvVoIPCallHistoryRemMediaIPAddr

(8) cCallHistoryCallOrigin

(9) cvCommonDcCallHistoryCoderTypeRate

For a complete description of these notifications and additional MIB functions, see the CISCO-VOICE-DIAL-CONTROL-MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs.

The **snmp-server enable traps voice** 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 SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable the router to send poor-quality-of-voice informs to the host at the address myhost.cisco.com using the community string defined as public:

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

The following example shows how to enable the router to send PSTN fallback messages at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server enable traps voice poor-qov	Enables poor quality-of-voice SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface which an SNMP trap should originate from.

snmp-server enable traps voice poor-qov

The **snmp-server enable traps voice poor-qov** command is replaced by the **snmp-server enable traps voice** command. See the **snmp-server enable traps voice** command for more information.