

Tech Note Cisco IOS SNMP Traps Supported and How to Conf

Table of Contents

<u>Cisco IOS SNMP Traps Supported and How to Configure Them</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Components Used</u>	2
<u>snmp-server host Command</u>	2
<u>Syntax Description</u>	2
<u>Examples</u>	6
<u>Defaults</u>	6
<u>Command Modes</u>	6
<u>Usage Guidelines</u>	8
<u>snmp-server enable traps Command</u>	8
<u>Syntax Description</u>	9
<u>Defaults</u>	17
<u>Command Modes</u>	17
<u>Usage Guidelines</u>	18
<u>Related Information</u>	19

Cisco IOS SNMP Traps Supported and How to Configure Them

Introduction

Before You Begin

- Conventions

- Prerequisites

- Components Used

snmp-server host Command

- Syntax Description

Defaults

Command Modes

Usage Guidelines

- Examples

snmp-server enable traps Command

- Syntax Description

Defaults

Command Modes

Usage Guidelines

Related Information

Introduction

Note: The Cisco IOS® Software used to prepare this document is Cisco IOS Software version 12.1(3)T. Please be aware that not all listed [notification-type] options are supported when you use an earlier Cisco IOS Software version. Also, when using versions higher than 12.1(3)T, additional [notification-type] options may be supported. A current list of all supported Cisco IOS Software Simple Network Management Protocol (SNMP) trap Object Identifiers (OIDs) can be found [here](#).

Cisco devices that run Cisco's standard IOS Software (routers, Asynchronous Transfer Mode (ATM) switches and Remote Access Servers) can generate many SNMP traps

Before You Begin

Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

Prerequisites

Readers of this document should be knowledgeable of the following:

In general, you probably don't want a Cisco device to send all the SNMP traps that it knows how to send. For instance, if you enable all traps in a Remote Access Server with 64 dial-in lines, you'll get a trap whenever a user dials in and whenever they terminate the connection. This creates too many traps. Fortunately, the Cisco IOS Software defines groups of traps that you can enable or disable. There are two global configuration commands that are used to configure SNMP traps into a Cisco IOS Software device:

-

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

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

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

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

The above commands are confusing, because the types of traps to be sent can be specified in both commands. The basic thing to do is to use the **snmp-server host** command to define the Network Management Systems to which traps are to be sent. You should also specify the trap types if you don't want all traps to be sent. Then use multiple **snmp-server enable traps** commands, one for each of the trap types that you used in the snmp host command.

**Note:** Not all [notification-type] options are supported on both of the above commands. For example, [notification-type] x25 and teletype (tty) are not used for **snmp-server enable trap**. x25 and tty traps are enabled by default.

As an example, to make a Cisco IOS Software device report only configuration, Border Gateway Protocol (BGP), and tty traps to Network Management System 10.10.10.10, use the following commands:

```
snmp-server host 10.10.10.10 public config bgp tty
snmp-server enable traps config
snmp-server enable traps bgp
```

## Components Used

This document is not restricted to specific software and hardware versions.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## snmp-server host Command

To specify the recipient of an SNMP notification operation, use the snmp-server host global configuration command. 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]]]
no snmp-server host host [traps | informs]
```

## Syntax Description

|           |                                                                |
|-----------|----------------------------------------------------------------|
| host-addr | Name or Internet address of the host (the targeted recipient). |
| traps     | (Optional) Send SNMP traps to this host. This is the default.  |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>informs</b>              | Optional) Send SNMP informs to this host.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>version</b>              | <p>(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model, as it allows packet encryption with the priv keyword. If you use the version keyword, one of the following must be specified:</p> <ul style="list-style-type: none"> <li>• <b>1</b> --SNMPv1. This option is not available with informs.</li> <li>• <b>2c</b> --SNMPv2C.</li> <li>• <b>3</b> --SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> <li>◆ <b>auth</b> (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication</li> <li>◆ <b>noauth</b> (Default). The noAuthNoPriv security level. This is the default if the [auth   noauth   priv] keyword choice is not specified.</li> <li>◆ <b>priv</b> (Optional). Enables Data Encryption Standard (DES) packet encryption (also called "privacy").</li> </ul> </li> </ul> |
| <i>community-string</i>     | <p>Password-like community string sent with the notification operation. Though you can set this string using the <b>snmp-server host</b> command by itself, we recommend that you define this string using the <b>snmp-server community</b> command prior to using the <b>snmp-server host</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>udp-port</b> <i>port</i> | User Datagram Protocol (UDP) port of the host to use. The default is 162.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| notification-type           | <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"> <li>• <b>aaa-server</b>--Sends AAA notifications.</li> <li>•</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**bgp**—Sends Border Gateway Protocol (BGP) state change notifications.

- **bstun**—Sends Block Serial Tunneling (BSTUN) notifications
- **calltracker**—Sends CallTracker notifications
- **config**—Sends configuration notifications.
- **dlsw**—Sends data-link switching (DLSw) notifications.
- **ds0-busyout**—Sends ds0-busyout notifications
- **ds1-loopback**—Sends ds1-loopback notifications
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **dsp**—Sends digital signal processing (DSP) notifications
- **entity**—Sends Entity Management Information Base (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.

- **msdp**—Sends Multicast Source Discovery Protocol (MSDP) notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) 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.
- **snmp**—Sends Simple Network Management Protocol (SNMP) notifications (as defined in RFC 1157).
- **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 voice notifications

|  |                                                                                                                                                                                          |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• <b>x25</b>—Sends X.25 event notifications.</li> <li>• <b>xgcp</b>—Sends External Media Gateway Control Protocol (XGCP) notifications</li> </ul> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Defaults

The **snmp-server host** 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:** Note: If the *community-string* 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 Software version 12.0(3) and later.

## Command Modes

Cisco IOS Software Release

Modification

10.0

Command introduced.

12.0(3)T

The following keywords have been added:

- **version 3 [auth | noauth | priv]**
- **hsrp**

## 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 protocol data unit (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 is taken into account. 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 replaces 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.

## Configuring Informs

To be able to send an inform, you need to perform the following steps:

1. Configure a remote engine ID.
2. Configure a remote user.
3. Configure a group on a remote device.
4. Enable traps on the remote device.
5. Enable the SNMP manager.

## 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:

```
snmp-server community comaccess ro 10
snmp-server host 172.20.2.160 comaccess
access-list 10 deny any
```

The following example sends the SNMP traps 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
```

The following example sends HSRP SNMPv2c traps to the host specified by the name myhost.cisco.com. The community string is defined as public.

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

## snmp-server enable traps Command

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

```
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. If no type is specified, all notifications are sent (including the <b>envmon</b> and <b>repeater</b> notifications). The notification type can be one of the following keywords:</p> <ul style="list-style-type: none"><li>• <b>aaa-server</b>—Sends AAA Server notifications. This keyword is added since Cisco IOS Software version 12.1(3)T for Cisco AS5300 and AS5800 platforms only. This is from the CISCO-AAA-SERVER-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.4.1.9.10.56.2<br/><br/>1 casServerStateChange</li><li>• <b>bgp</b>—Sends Border Gateway Protocol (BGP) state change notifications. This is from the BGP4-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.2.1.15.7<br/><br/>1 bgpEstablished<br/><br/>2 bgpBackwardTransition</li><li>• <b>calltracker</b>—Sends notification whenever a new active call entry is created in the cctActiveTable or a new history call entry is created in the cctHistoryTable This is from the CISCO-CALL-TRACKER-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.4.1.9.9.163.2<br/><br/>1 cctCallSetupNotification<br/><br/>2 cctCallTerminateNotification</li><li>• <b>config</b>—Sends configuration notifications. This is from the CISCO-CONFIG-MAN-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.4.1.9.9.43.2</li></ul> |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

1 ciscoConfigManEvent

- **dial**—Sends notification whenever a successful call clears, a failed call attempt is determined to have ultimately failed, or whenever a call setup message is received or sent. This is from the DIAL-CONTROL-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.2.1.10.21.2

1 dialCtlPeerCallInformation

2 dialCtlPeerCallSetup

- **dls**—Sends notifications from DLSw agents  
When the **dls** keyword is used, you can specify a *notification-option* value. This is from the CISCO-DLSW-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.10.9.1.7

1 ciscoDlswTrapTConnPartnerReject

2 ciscoDlswTrapTConnProtViolation

3 ciscoDlswTrapTConnUp

4 ciscoDlswTrapTConnDown

5 ciscoDlswTrapCircuitUp

6 ciscoDlswTrapCircuitDown

- **ds0-busyout**—Sends notification whenever the busyout of a DS0 interface changes state. This keyword is added since Cisco IOS Software version 12.1(3)T for the Cisco AS5300 platform only. This is from the CISCO-POP-MGMT-MIB-V1SMI.my and the notification is:

enterprise 1.3.6.1.4.1.9.10.19.2

1 cpmDS0BusyoutNotification

-

**ds1-loopback**—Sends notification whenever the DS1 interface goes into loopback mode. This keyword is added since Cisco IOS Software version 12.1(3)T for the Cisco AS5300 platform only. This is from the CISCO-POP-MGMT-MIB-V1SMI.my and the notification is:

```
enterprise 1.3.6.1.4.1.9.10.19.2
```

```
2 cpmDS1LoopbackNotification
```

- 

**dspu**—Sends notification whenever the operational state of the physical unit (PU) or the logical unit (LU) changes or activation failure is detected. This is from the CISCO-DSPU-MIB-V1SMI.my and the notifications are:

```
enterprise 1.3.6.1.4.1.9.9.24.1.4.4
```

```
1 newdspuPuStateChangeTrap
```

```
2 newdspuPuActivationFailureTrap
```

```
enterprise 1.3.6.1.4.1.9.9.24.1.5.3
```

```
1 newdspuLuStateChangeTrap
```

```
2 dspuLuActivationFailureTrap
```

- 

**dsp**—Sends notification whenever the DSP card is going up or down. This is from the CISCO-DSP-MGMT-MIB-V1SMI.my and the notification is:

```
enterprise 1.3.6.1.4.1.9.9.86.2
```

```
1 cdsMIBCardStateNotification
```

- 

**entity**—Sends Entity MIB modification notifications. This is from the ENTITY-MIB-V1SMI.my and the notifications are:

```
enterprise 1.3.6.1.2.1.47.2
```

```
1 entConfigChange
```

-

**envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded. When the **envmon** keyword is used, you can specify a *notification-option* value. This is from the CISCO-ENVMON-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.13.3

1 ciscoEnvMonShutdownNotification

2 ciscoEnvMonVoltageNotification

3 ciscoEnvMonTemperatureNotification

4 ciscoEnvMonFanNotification

5 ciscoEnvMonRedundantSupplyNotification

•

**frame-relay**—Sends Frame Relay notifications. This is from the RFC1315-MIB.my and the notifications are:

enterprise 1.3.6.1.2.1.10.32

1 frDLCIStatusChange

•

**hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications. This feature is supported since Cisco IOS Software version 12.0(3)T. This is from the CISCO-HSRP-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.106.2

1 cHsrpStateChange

•

**isdn**—Sends Integrated Services Digital Network (ISDN) notifications. When the **isdn** keyword is used, you can specify a *notification-option* value. This is from the CISCO-ISDN-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.26.2

1 demandNbrCallInformation

2 demandNbrCallDetails

3 demandNbrLayer2Change [supported since Cisco IOS Software version 12.1(1)T ]

4 demandNbrCNANotification [supported since Cisco IOS Software version 12.1(5)T ]

This is from the CISCO-ISDNU-IF-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.18.2

1 ciuIfLoopStatusNotification

- **msdp**—Sends Multicast Source Discovery Protocol (MSDP) notifications. This is from the MSDP-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.3.92.1.1.7

1 msdpEstablished

2 msdpBackwardTransition

- **repeater**—Sends Ethernet hub **repeater** notifications. When the repeater keyword is selected, you can specify a *notification-option* value. This is from the CISCO-REPEATER-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.22.3

1 ciscoRptrIllegalSrcAddrTrap

- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications. This feature is supported since Cisco IOS Software version 12.0(2)T. This is from the RSVP-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.3.71.2

1 newFlow

2 lostFlow

**rtr**—Sends Service Assurance Agent RTR (RTR) notifications. This is from the CISCO-RTTMON-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.42.2

1 rttMonConnectionChangeNotification

2 rttMonTimeoutNotification

3 rttMonThresholdNotification

- **snmp**—Sends Simple Network Management Protocol (SNMP) notifications. When the snmp keyword is used, you can specify a notification-option value. This is from the CISCO-GENERAL-TRAPS.my and the notifications are:

enterprise 1.3.6.1.2.1.11

0 coldStart

2 linkDown

3 linkUp

4 authenticationFailure

5 egpNeighborLoss

enterprise 1.3.6.1.4.1.9

0 reload

**Note:** The following trap is controlled by the notification-type "tty":

**Note:** 1 tcpConnectionClose

- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. This is from the CISCO-SYSLOG-MIB-V1SMI.my and the notifications are:

enterprise 1.3.6.1.4.1.9.9.41.2



|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|                            | <p>1 clogMessageGenerated</p> <ul style="list-style-type: none"> <li>• <b>voice</b>—Sends poor quality of voice notification. This is from the CISCO-VOICE-DIAL-CONTROL-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.4.1.9.9.63.2<br/><br/>1 cvdcPoorQoVNotification</li> <li>• <b>xgcp</b>—Sends External Media Gateway Control Protocol (XGCP) notifications. This is from the XGCP-MIB-V1SMI.my and the notifications are:<br/><br/>enterprise 1.3.6.1.3.90.2<br/><br/>1 xgcpUpDownNotification</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |  |
| <i>notification-option</i> | <p>(Optional)</p> <ul style="list-style-type: none"> <li>• <b>dls w [circuit   tconn]</b> -- When the <b>dls w</b> keyword is used, you can specify the specific notification type you wish to enable or disable. If no keyword is used, all DLSw notification types are enabled. The option can be one or more of the following keywords: <ul style="list-style-type: none"> <li>◆ <b>circuit</b>—Enables DLSw circuit traps.</li> <li>◆ <b>tconn</b>—Enables DLSw peer transport connection traps.</li> </ul> </li> <li>• <b>envmon [voltage   shutdown   supply   fan   temperature]</b> --When the <b>envmon</b> 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: <b>voltage</b>, <b>shutdown</b>, <b>supply</b>, <b>fan</b>, and <b>temperature</b>.</li> <li>• <b>isdn [call-information   isdn u-interface  </b></li> </ul> |  |

**chan-not-avail | layer2]** --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 one or more of the following keywords:  
health--Enables Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification. reset--Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

- ◆ **health**--Enables Internet Engineering Task Force (IETF) Repeater Hub MIB (RFC 1516) health notification.

- ◆ **reset**--Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

- **snmp [authentication | linkup | linkdown | coldstart]** keywords **linkup | linkdown | coldstart** added since Cisco IOS Software version 12.1(3)T. -- When the **snmp** keyword is used, you can specify the specific notification type you wish to enable or disable. If no keyword is used, all SNMP notification types are enabled (or disabled, if the no form is used). The notification types available are:

- ◆ **authentication**--Controls the sending of SNMP authentication failure notifications. An authenticationFailure(4) trap signifies that the sending protocol entity is the addressee of a protocol message that is not properly authenticated.

- ◆

**linkup**—Controls the sending of SNMP linkup notifications. A linkUp(3) trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.

◆  
**linkdown**—Controls the sending of SNMP linkdown notifications. A linkDown(2) trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.

◆  
**coldstart**—Controls the sending of SNMP coldstart notifications. A coldStart(0) trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.

## Defaults

SNMP notifications are disabled.

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

## Command Modes

Release

Modification

11.1

This command was introduced.

12.0(2)T

The **rsvp** keyword was added.

12.0(3)T

The **hsrp** keyword was added.

12.1(3)T

The following keywords have been added to the **snmp-server enable traps snmp** form of this command:

- **linkup**
- **linkdown**
- **coldstart**

The following notification type keywords have been added for the Cisco AS5300 platform only:

- **ds0-busyout**
- **isdn chan-not-avail**
- **modem-health**
- **ds1-loopback**

The following notification type keyword has been added for the Cisco AS5300 and AS5800 platforms only:

- **aaa-server**

## Usage Guidelines

The **snmp-server enable traps snmp [ linkup ] [linkdown]** form of this command replaces the **snmp trap link-status** interface configuration mode command.

The **no** form of the **snmp-server enable traps** command is useful for disabling notifications that are generating a large amount of unneeded noise on your network.

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. In order 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. In order 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. 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, 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 enabled or disabled (for example, HSRP traps are defined using the HSRP MIB, repeater traps are defined using the Repeater Hub MIB, and so on). Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these cannot be controlled using the **snmp-server enable** command.

---

## Related Information

- [Configuring Extended ATM PVC Trap Support](#)
- [Technical Support – Cisco Systems](#)

---

All contents are Copyright © 1992–2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Dec 23, 2002

Document ID: 13506

---