snmp-server engineID local through snmp trap link-status

snmp-server file-transfer access-group

To associate an access list to the transfer protocols TFTP, FTP, Remote Copy Protocol (RCP), Secure Copy Protocol (SCP), and Secured File Transfer Protocol (SFTP), use the **snmp-server file-transfer access-group** command in global configuration mode. To disassociate an access list, use **no** form of this command.

snmp-server file-transfer access-group {*acl-number*| *acl-name*} [**protocol** *p-name*]

no snmp-server file-transfer access-group {*acl-number*| *acl-name*}

Syntax Description

acl-number	Integer from 1 to 99 that specifies a standard ACL.
acl-name	String that specifies a standard ACL.
protocol	(Optional) Enables the user to associate a named protocol with an access group.
p-name	(Optional) Name of a transfer protocol. Valid values are: **ftp**, **rcp**, **scp**, **sftp**, and **tftp**.

Command Default

If a protocol is not specified, all protocols are associated with the access list.

Command Modes

Global configuration

Command History

Release	Modification
12.4(12)	This command was introduced. This command replaces the **snmp-server tftp-server-list** command.

Usage Guidelines

The **snmp-server tftp-server-list** command is still supported in Cisco IOS software, but if it is configured as **snmp-server tftp-server-list 10**, it will be substituted with the **snmp-server file-transfer access-group 10 protocol tftp**command.

Use the **snmp-server file-transfer access-group**command to restrict configuration transfers that are initiated via Simple Network Management Protocol (SNMP). You can restrict transfers for specific transfer protocols by associating an access list to the protocol.

Examples

The following example associates access group 10 to the transfer protocols FTP and RCP:

```
Router(config)# snmp-server file-transfer access-group 10 protocol ftp
Router(config)# snmp-server file-transfer access-group 10 protocol rcp
```

Related Commands

Command	Description
snmp-server tftp-server-list	Associates TFTP servers used via SNMP controlled TFTP operations to the servers specified in an access list.

snmp-server ip dscp

To set the IP Differentiated Services Code Point (DSCP) value for Simple Network Management Protocol (SNMP) traffic, use the **snmp-server ip dscp** command in global configuration mode. To disable the configured value, use the **no** form of this command.

snmp-server ip dscp *value*

no snmp-server ip dscp *value*

Syntax Description

value	The IP DSCP value to apply to SNMP traffic. Valid values for IP DSCP are 0 through 63. The default is 0.

Command Default

The IP DSCP default value for SNMP traffic is 0.

Command Modes

Global config

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify an IP DSCP value to give SNMP traffic higher or lower priority in your network.

The following example shows how to set the IP DSCP value to 45:

```
Router(config)# snmp-server ip dscp 45
```

Related Commands

Command	Description
snmp-server ip precedence	Configures the IP Precedence value.

snmp-server ip precedence

snmp-server ip precedence *value*

no snmp-server ip precedence *value*

Syntax Description

value	The IP Precedence value to apply to SNMP traffic. Valid values for IP Precedence are 0 through 7. The default is 0.

Command Default

The IP Precedence default value for SNMP traffic is 0.

Command Modes

Global config.

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify an IP Precedence value to give SNMP traffic higher or lower priority in your network.

Examples

The following example shows how to set the IP Precedence value to 7:

```
Router(config)# snmp-server ip precedence
 7
```

Related Commands

Command	Description
snmp-server ip dscp	Configures the IP DSCP value.

snmp-server manager

To start the Simple Network Management Protocol (SNMP) manager process, use the **snmp-server manager**command in global configuration mode. To stop the SNMP manager process, use the **no** form of this command.

snmp-server manager

no snmp-server manager

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.

Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.

SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162.

Examples

The following example shows how to enable the SNMP manager process:

```
Router(config)# snmp-server manager
```

Related Commands

Command	Description
show snmp	Checks the status of SNMP communications.
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager session-timeout	Sets the amount of time before a nonactive session is destroyed.

snmp-server manager session-timeout

To set the amount of time before a nonactive session is destroyed, use the **snmp-server manager session-timeout** command in global configuration mode. To return the value to its default, use the **no** form of this command.

snmp-server manager session-timeout *seconds*

no snmp-server manager session-timeout

Syntax Description

seconds	Number of seconds before an idle session is timed out. The default is 600.

Command Default

Idle sessions time out after 600 seconds (10 minutes).

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	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.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS Release XE 2.1.

Usage Guidelines

Sessions are created when the SNMP manager in the router sends SNMP requests, such as inform requests, to a host or receives SNMP notifications from a host. One session is created for each destination host. If there is no further communication between the router and host within the session timeout period, the session will be deleted.

The router tracks statistics, such as the average round-trip time required to reach the host, for each session. Using the statistics for a session, the SNMP manager in the router can set reasonable timeout periods for future requests, such as informs, for that host. If the session is deleted, all statistics are lost. If another session with the same host is later created, the request timeout value for replies will return to the default value.

However, sessions consume memory. A reasonable session timeout value should be large enough such that regularly used sessions are not prematurely deleted, yet small enough such that irregularly used, or one-shot sessions, are purged expeditiously.

Examples

The following example shows how to set the session timeout to a larger value than the default:

```
Router(config)# snmp-server manager
Router(config)# snmp-server manager session-timeout 1000
```

Related Commands

Command	Description
show snmp pending	Displays the current set of pending SNMP requests.
show snmp sessions	Displays the current SNMP sessions.
snmp-server manager	Starts the SNMP manager process.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** command in global configuration mode.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied. The default is 10.

Command Default

The queue length is set to 10.

Command Modes

Global configuration

Command History

Release	Modification
10.0	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 defines the length of the message queue for each trap host. When a trap message is successfully transmitted, Cisco IOS software will continue to empty the queue but never faster than at a rate of four trap messages per second.

During device bootup, some traps could be dropped because of trap queue overflow on the device. If you think that traps are being dropped, you can increase the size of the trap queue (for example, to 100) to determine if traps can then be sent during bootup.

Examples

The following example shows how to set the Simple Network Management Protocol (SNMP) notification queue to 50 events:

```
Router(config)# snmp-server queue-length 50
```

Related Commands

Command	Description
snmp-server packetsize	Establishes control over the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.

snmp-server queue-limit

To establish the message queue size for various queues, use the **snmp-server queue-limit** command in global configuration mode. To disable the configured settings, use the **no** form of this command.

snmp-server queue-limit {**dispatcher**| **engine**| **notification-host**} *queue-length*

no snmp-server queue-limit {**dispatcher**| **engine**| **notification-host**}

Syntax Description

dispatcher	Specifies the SNMP PDU dispatcher queue length.
engine	Specifies the SNMP engine queue length.
notification-host	Specifies the message queue length for each notification host.
queue-length	Length of the queue. The range for **dispatcher** and **engine** is 1 to 1000. The range for **notification-host** is 1 to 5000. The default *queue-length* value for notification-host is 10.

Command Default

By default, message queue size is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(33)S	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. The range of queue length for notification host was changed to 1 to 5000.

Usage Guidelines

Use the **snmp-server queue-limit** command to set the message queue size for different queues. Using this command you can resize the queue for dispatcher, engine, and host traps.

Examples

The following example shows how to set the message queue length of each notification host to 50:

```
Router(config)# snmp-server queue-limit notification-host 50
```

Related Commands

Command	Description
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server source-interface

To specify the interface from which a Simple Network Management Protocol (SNMP) trap originates the informs or traps, use the **snmp-server source-interface** command in global configuration mode. To remove the source designation, use the **no** form of this command.

snmp-server source-interface {**traps**| **informs**} *interface*

no snmp-server source-interface {**traps**| **informs**} [*interface*]

Syntax Description

traps	Specifies SNMP traps.
informs	Specifies SNMP informs.
interface	The interface type and the module and port number of the source interface.

Command Default

No interface is designated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXB2	This command was introduced.
12.2(18)SXF6	The **informs** keyword was added. This command replaced the **snmp-server trap-source**command.
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 replaced the **snmp-server trap-source**command.

Note The **snmp-server trap-source**command is available in other versions of Cisco IOS software for backward compatibility.

The source interface must have an IP address. Enter the *interface* argument in the following format: *interface-type module* / *port*.

An SNMP trap or inform sent from a Cisco SNMP server has a notification IP address of the interface it went out of at that time. Use this command to monitor notifications from a particular interface.

Examples

The following example shows how to specify that Gigabit Ethernet interface 5/2 is the source for all informs:

```
snmp-server source-interface informs gigabitethernet5/2
```

The following example shows how to specify that the Gigabit Ethernet interface 5/3 is the source for all traps:

```
snmp-server source-interface traps gigabitethernet5/3
```

The following example shows how to remove the source designation for all traps for a specific interface:

```
no snmp-server source-interface traps gigabitethernet5/3
```

Related Commands

Command	Description
snmp-server enable traps	Enables a router to send SNMP traps and informs.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which a SNMP trap should originate.

snmp-server trap authentication unknown-context

To enable the Simple Network Management Protocol (SNMP) authorization failure (authFail) traps during an unknown context error, use the **snmp-server trap authentication unknown-context** command in global configuration mode. To disable the authFail traps, use the **no** form of this command.

snmp-server trap authentication unknown-context

no snmp-server trap authentication unknown-context

Syntax Description

This command has no arguments or keywords.

Command Default

No authFail traps are generated.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
12.4(22)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(22)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to enable the authorization failure traps during an unknown context error:

```
Router(config)# snmp-server trap authentication unknown-context
```

The following example shows how to disable the authorization failure traps during an unknown context error:

```
Router(config)# no snmp-server trap authentication unknown-context
```

snmp-server trap authentication vrf

To enable virtual private network (VPN) routing and forwarding (VRF) instance context authentication notifications, use the **snmp-server trap authentication vrf**command in global configuration mode. To suppress authentication notifications for Simple Network Management Protocol (SNMP) packets dropped due specifically to VRF context mismatches while keeping all other SNMP authentication notifications enabled, use the **no** form of this command.

snmp-server trap authentication vrf

no snmp-server trap authentication vrf

Syntax Description

This command has no arguments or keywords.

Command Default

No VRF-specific authentication notifications are enabled when SNMP authentication notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Release 12.3(2)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The **snmp-server enable traps snmp authentication**command controls SNMP authentication traps and the **no** form of this command disables all SNMP authentication failure notifications. The **snmp-server trap authentication vrf** command provides more granular control of these notifications.

With context-based MIB access, SNMP requests on each VRF are tied to a specific context. This context is used for access control. If SNMP contexts are configured for VPNs, any SNMP request not matching the configured context will generate an SNMP authentication failure notification.The **no snmp-server trap**

authentication vrf command allows you to suppress the authentication failure notifications that are specific to these VRF contexts, while keeping all other SNMP authentication failure notifications enabled.

The **no snmp-server trap authentication vrf** command has no effect if the **snmp-server enable traps snmp authentication**command has not been configured..

Examples

The following example shows how to enable a router to send SNMP authentication traps to host myhost.cisco.com using the community string public while disabling all VRF authentication traps:

```
Router(config)# snmp-server enable traps snmp authentication

Router(config)# no snmp-server trap authentication vrf
Router(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
snmp-server enable traps snmp	Enables the sending of RFC 1157 SNMP notifications.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server trap link

To enable linkUp/linkDown Simple Network Management Protocol (SNMP) traps that are compliant with RFC2233, use the **snmp-server trap link** command in global configuration mode. To disable IETF- compliant functionality and revert to the default Cisco implementation of linkUp/linkDown traps, use the **no** form of this command.

snmp-server trap link ietf

no snmp-server trap link ietf

Syntax Description

ietf	Notifies the command parser to link functionality of SNMP linkUp/linkDown traps to the Internet Engineering Task Force (IETF) standard (instead of the previous Cisco implementation).

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(2)T	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

The **snmp-server trap link ietf** command is used to configure your router to use the RFC2233 IETF standards-based implementation of linkUp/linkDown traps. This command is disabled by default to allow you to continue using the earlier Cisco implementation of linkUp/linkDown traps if you so choose.

However, please note that when using the default Cisco object definitions, linkUp/linkDown traps are not generated correctly for sub-interfaces. In the default implementation an arbitrary value is used for the *locIfReason* object in linkUp/linkDown traps for sub-interfaces, which may give you unintended results. This is because the *locIfReason* object is not defined for sub-interfaces in the current Cisco implementation, which uses OLD-CISCO-INTERFACES-MIB.my.

If you do not enable this functionality, the link trap varbind list will consist of {ifIndex, ifDescr, ifType, locIfReason}. After you enable this functionality with the **snmp-server trap link ietf** command, the varbind list will consist of {inIndex, ifAdminStatus,ifOperStatus, if Descr, ifType}. The *locIfReason* object will also

be conditionally included in this list depending on whether meaningful information can be retrieved for that object. A configured sub-interface will generate retrievable information. On non-HWIDB interfaces, there will be no defined value for *locIfReason* , so it will be omitted from the trap message.

Examples

The following example shows the enabling of the RFC 2233 linkUp/linkDown traps, starting in privileged EXEC mode:

```
Router#
configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
snmp-server trap link ietf

Router(config)#
end
Router#
 more system:running configuration
.
.
.
!
snmp-server engineID local 00000009000000A1616C2056
snmp-server community public RO
snmp-server community private RW
snmp-server trap link ietf
!
.
.
.
```

Related Commands

Command	Description
debug snmp packets	Displays information about every SNMP packet sent or received by the router for the purposes of troubleshooting.

snmp-server trap link switchover

To enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover, use the **snmp-server trap link switchover** command in global configuration mode. To disable linkdown during a switch failover, use the **no** form of this command.

snmp-server trap link switchover

no snmp-server trap link switchover

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF2	This command was introduced on the Supervisor Engine 720 and the Supervisor Engine 32.
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

By default, no link traps are generated during a switchover.

Examples

This example shows how to enable sending a linkdown trap followed by a linkup trap for every interface in the switch during a switch failover:

```
snmp-server trap link switchover
```

This example shows how to disable linkdown followed by a linkup trap for every interface in the switch during a switch failover:

```
no snmp-server trap link switchover
```

snmp-server trap retry

To define the number of times the Simple Network Management Protocol (SNMP) agent on a device tries to find a route before it sends traps, use the **snmp-server trap retry** command in global configuration mode.

snmp-server trap retry *number*

Syntax Description

number	Integer from 0 to 10 that sets the number of times the message will be retransmitted. The default is 3.

Command Default

Messages are not retransmitted.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The SNMP agent looks for a configured route in the system before sending a trap out to a destination. If a route is not present, traps are queued in the trap queue and discarded when the queue becomes full. When the **snmp-server trap retry** command is configured, the route search retry number tells the agent how many times to look for the route before sending the trap out.

Configuring the **snmp-server trap retry** command also ensures that policy-based routing traps are sent and not discarded. Policy-based traps must be sent immediately and routes are not needed. The number of retries must be set to 0 so that policy-based traps are sent immediately.

Examples

The following example shows how to set the number of times a SNMP agent on a device tries to find a route to 10:

```
Router(config)# snmp-server trap retry 10
```

Related Commands

Command	Description
snmp-server trap timeout	Defines an interval of time between retransmissions of traps on a retransmission queue.

snmp-server trap timeout

To define an interval of time between retransmissions of trap messages on a retransmission queue, use the **snmp-server trap timeout** command in global configuration mode.

snmp-server trap timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

This command is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRA	This command was introduced. This command replaces the **snmp-server trap-timeout** command in Cisco IOS Release 12.2SR only.

Usage Guidelines

Before a trap is sent, the SNMP agent looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. Issue the **snmp-server trap timeout** command to configure the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between retransmissions of traps:

```
Router(config)# snmp-server trap timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server trap-authentication

The **snmp-server trap-authentication** command has been replaced by the **snmp-server enable traps snmp authentication** command. See the description of the **snmp-server enable traps snmp** command in this chapter for more information.

snmp-server trap-timeout

Note This command is not supported in Cisco IOS Release 12.2SR. For Cisco IOS Release12.2SR, use the **snmp-server trap timeout** command.

To define an interval of time before resending trap messages on the retransmission queue, use the **snmp-server trap-timeout** command in global configuration mode.

snmp-server trap-timeout *seconds*

Syntax Description

seconds	Integer from 1 to 1000 that sets the interval, in seconds, for resending messages. The default is 30.

Command Default

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was replaced by the **snmp-server trap timeout** command in Cisco IOS Release 12.2SR.

Usage Guidelines

The **snmp-server trap-timeout** command remains in Cisco IOS software for compatibility but is written in the configuration as **snmp-server trap timeout**.

Before the Cisco IOS software tries to send a trap, it looks for a route to the destination address. If there is no known route, the trap is saved in a retransmission queue. The **snmp-server trap-timeout** command determines the number of seconds between retransmission attempts.

Examples

The following example shows how to set an interval of 20 seconds between resending trap messages on the retransmission queue:

```
Router(config)# snmp-server trap-timeout 20
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server queue-length	Establishes the message queue length for each trap host.

snmp-server usm cisco

To enable Cisco-specific error messages for Simple Network Management Protocol Version 3 (SNMPv3), which is a User-based Security Model (USM), use the **snmp-server usm cisco** command in global configuration mode. To disable the Cisco-specific error messages for SNMPv3 USM, use the **no** form of this command.

snmp-server usm cisco

no snmp-server usm cisco

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco-specific error messages for SNMPv3 USM are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

The RFC 3414-compliant error messages are descriptive and can lead to misuse of information by malicious users. Use the **snmp-server usm cisco** command to enable Cisco-specific messages that help to hide the exact error condition. Enabling Cisco-specific messages for SNMPv3 is a deviation from RFC 3414.

Examples

The following example shows how to enable the Cisco-specific error messages for SNMPv3 USM:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server usm cisco
Router(config)# exit
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class.

snmp trap if-monitor

To enable if-monitor traps for a particular interface, use the **snmp trap if-monitor**command in interface configuration mode. To disable traps on an interface, use the **no** form of this command.

snmp trap if-monitor

no snmp trap if-monitor

Syntax Description

This command has no arguments or keywords.

Command Default

Traps are not generated.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

Traps are sent for the interface only if they have been enabled globally by issuing the **snmp-server enable traps if-monitor** command and then explicitly on that interface by issuing the **snmp trap if-monitor**command.

Examples

The following example shows how to enable if-monitor traps on a specific interface:

```
Router(config)# snmp-server enable traps if-monitor
Router(config)# interface ethernet 1/1
Router(config-if)# snmp trap if-monitor
```

Related Commands

Command	Description
snmp-server enable traps if-monitor	Globally enables if-monitor traps.

snmp trap link-status

To enable Simple Network Management Protocol (SNMP) link trap generation, use the **snmp trap link-status** command in either interface configuration mode or service instance configuration mode. To disable SNMP link trap generation, use the **no** form of this command.

snmp trap link-status [**permit duplicates**]

no snmp trap link-status [**permit duplicates**]

Syntax Description

permit duplicates	(Optional) Permits duplicate SNMP linkup and linkdown traps.

Command Default

SNMP link traps are generated when an interface goes up or down.

Command Modes

Interface configuration (config-if) Service instance configuration (config-if-srv)

Command History

Release	Modification
10.0	This command was introduced.
12.2(30)S	This command was modified. The **permit duplicates** keyword pair was added.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
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.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4 as described in the Usage Guidelines.
12.2(33)SRD1	Support for this command was extended to service instance configuration mode.
12.2(33)SRE6	This command was modified. This command must be enabled on each subinterface from this release onwards.
15.1(3)S3	This command was integrated into Cisco IOS Release 15.1(3)S3.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces such as ISDN interfaces, expected to go up and down during normal usage, the output generated by these traps may not be useful. The **no** form of this command disables these traps.

The **permit** and **duplicates** keywords are used together and cannot be used individually. Use the **permit duplicates** keyword pair when an interface is not generating SNMP linkup traps, linkdown traps, or both. When the **snmp trap link-status permit duplicates** command is configured, more than one trap may be sent for the same linkup or linkdown transition.

The **permit duplicates** keyword pair does not guarantee that SNMP link traps will be generated nor should configuring these keywords be required to receive traps.

By default, in service instance configuration mode, SNMP link traps are not sent. Also, the **permit duplicates** keyword pair is not available in service instance configuration mode.

The **snmp trap link-status** command must be used in conjunction with the **snmp-server enable traps atm subif** command in order to enable SNMP trap notifications on ATM subinterfaces. The **snmp-server enable traps atm subif** command must be configured in global configuration mode, and then the **snmp trap link-status** command must be configured on each ATM subinterface for which you want to enable SNMP trap notifications.

Cisco 10000 Series Router

In Cisco IOS Release 12.2(33)SB, the **virtual-template snmp** command has a new default configuration. Instead of being enabled by default, **no virtual-template snmp** is the default configuration. This setting enhances scaling and prevents large numbers of entries in the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs.

If you configure the **no virtual-template snmp** command, the device no longer accepts the **snmp trap link-status** command under a virtual-template interface. Instead, the device displays a configuration error message such as the following:

```
Device(config)# interface virtual-template 1
Device(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the device reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

The following example shows how to disable SNMP link traps related to the ISDN BRI interface 0:

```
Device(config)# interface bri 0
Device(config-if)# no snmp trap link-status
```

The following example shows how to enable SNMP link traps for service instance 50 on Ethernet interface 0/1:

```
Device(config)# interface ethernet 0/1
Device(config-if)# service instance 50 ethernet
Device(config-if-srv)# snmp trap link-status
Device(config-if-srv)# end
```

Related Commands

Command	Description
snmp-server enable traps atm subif	Enables the sending of ATM subinterface SNMP notifications.
virtual-template snmp	Allows virtual access interfaces to register with SNMP when they are created or reused.