SNMP Commands

This chapter contains the Cisco ONS 15540 ESPx-specific SNMP commands. For the complete list of SNMP commands supported on the Cisco ONS 15540 ESPx, and their descriptions, refer to *Cisco IOS Configuration Fundamentals Command Reference* publication.

snmp-server enable traps aps

To enable SNMP trap notifications for APS activity, use the **snmp-server enable traps aps** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps aps

no snmp-server enable traps aps

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the APS MIB (CISCO-APS-MIB).

The **snmp-server enable traps aps** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for APS activity, the **snmp-server enable traps aps** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps aps
```

Related Commands

Command	Description
associate interface	Specifies interfaces to be associated and enters APS configuration mode.
show aps	Displays APS configuration information and status.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps cdl

To enable SNMP trap notifications defined in CISCO-CDL-MIB, use the **snmp-server enable traps cdl** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

no snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

Syntax Description

all	Enables trap notifications on all in-band message channel capable interfaces.
terminating-interfaces	Enables trap notifications only on terminating interfaces for in-band message channel traffic.
soak-interval	Sets interval after which trap notifications are sent.
set-soak-interval	Indicates time interval in milliseconds before sending defect indication trap notifications when a defect is set. The range is 100 to 60,000.
clear-soak-interval	Indicates time interval in milliseconds before sending defect indication trap notifications when a defect is cleared. The range is 100 to 60,000.

Defaults

Disabled

Set interval: 2500 milliseconds

Clear interval: 10,000 milliseconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the in-band message channel MIB (CISCO-CDL-MIB). SNMP trap notifications are sent when an in-band message channel connection is created, modified, or deleted.

The soak interval prevents the system from being flooded with set and clear notifications for defect indications. The default values for the soak interval are adequate for most network topologies.

The **snmp-server enable traps cdl** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps cdl** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps patch

To enable SNMP trap notifications for patch connection activity, use the **snmp-server enable traps patch** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps patch

no snmp-server enable traps patch

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the OSCP MIB (CISCO-OPTICAL-PATCH-MIB). SNMP trap notifications are sent when a patch connection is created, modified, or deleted.

The **snmp-server enable traps patch** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps patch** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps patch
```

Related Commands

Command	Description
patch	Configures patch connections.
show patch	Displays patch connection information.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps cdl

To enable SNMP trap notifications defined in CISCO-CDL-MIB, use the **snmp-server enable traps cdl** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

no snmp-server enable traps cdl {**all** | **terminating-interfaces**} [**soak-interval** *set-soak-interval clear-soak-interval*]

Syntax Description

all	Enables trap notifications on all in-band message channel capable interfaces.
terminating-interfaces	Enables trap notifications only on terminating interfaces for in-band message channel traffic.
soak-interval	Sets interval after which trap notifications are sent.
set-soak-interval	Specifies time interval in milliseconds before sending defect indication trap notifications when a defect is set. The range is 100 to 60,000.
clear-soak-interval	Specifies time interval in milliseconds before sending defect indication trap notifications when a defect is cleared. The range is 100 to 60,000.

Defaults

Disabled

Set interval: 2500 milliseconds

Clear interval: 10,000 milliseconds

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV2	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the in-band message channel MIB (CISCO-CDL-MIB). SNMP trap notifications are sent when an in-band message channel connection is created, modified, or deleted.

The soak interval prevents the system from being flooded with set and clear notifications for defect indications. The default values for the soak interval are adequate for most network topologies.

The **snmp-server enable traps cdl** command is used in conjunction with the **snmp-server host** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps cdl** command and the **snmp-server host** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for patch connection activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps cdl all
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
snmp-server host	Specifies the recipient for SNMP notification messages.

snmp-server enable traps oscp

To enable SNMP trap notifications for OSCP activity, use the **snmp-server enable traps oscp** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps oscp

no snmp-server enable traps oscp

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the OSCP MIB (CISCO-OSCP-MIB).

The **snmp-server enable traps oscp** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for OSCP activity, the **snmp-server enable traps oscp** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for OSCP activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps oscp
```

Related Commands

Command	Description
show oscp info	Displays OSCP configuration information.
show oscp neighbor	Displays OSCP neighbor information.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps rf

To enable SNMP trap notification for processor card redundancy activity, use the **snmp-server enable traps rf** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps rf

no snmp-server enable traps rf

Syntax Description

This command has no other arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the Redundancy Facility MIB (CISCO-RF-MIB).

The **snmp-server enable traps patch** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for patch connection activity, the **snmp-server enable traps patch** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for processor card redundancy activity.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rf
```

Related Commands

Command	Description
redundancy	Enters redundancy configuration mode.
show redundancy summary	Displays redundancy configuration information and status.
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.

snmp-server enable traps threshold min-severity

To enable SNMP trap notifications for alarm thresholds, use the **snmp-server enable traps threshold min-severity** command. To disable this feature, use the **no** form of this command.

snmp-server enable traps threshold min-severity {**degrade** | **failure**}

no snmp-server enable traps threshold min-severity

Syntax Description

degrade	Specifies signal degrade as the minimum severity for SNMP trap notifications.
failure	Specifies signal failure as the minimum severity for SNMP trap notifications.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the alarm threshold MIB (CISCO-IF-THRESHOLD-MIB).

The **snmp-server enable traps threshold min-severity** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for alarm threshold activity, the **snmp-server enable traps threshold min-severity** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for alarm threshold activity and set the minimum severity to failure.

```
Switch# configure terminal
```

```
Switch(config)# snmp-server enable traps threshold min-severity failure
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
show threshold-list	Displays the contents of a threshold list.
traceroute	Specifies the recipient for SNMP notification messages.
threshold-list	Groups a set of thresholds with a name. Switches from configuration mode to threshold-list configuration mode.

snmp-server enable traps topology

To enable SNMP trap notifications for the network topology activity, use the **snmp-server enable traps topology** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps topology [**throttle-interval** *seconds*]

no snmp-server enable traps topology [**throttle-interval** *seconds*]

Syntax Description

throttle-interval *seconds*	Specifies the number of seconds for the throttle timer interval. Valid values are 5 through 3600 seconds. If this keyword is omitted, the command defaults to 60 seconds at bootup time, or to the previous value configured.

Defaults

Disabled

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

Use this command to enable the SNMP trap notifications defined in the physical topology MIB (PTOPO-MIB).

The network topology trap throttle timer prevents the system from flooding the network with messages. We recommend a 60-second interval value.

The **snmp-server enable traps topology** command is used in conjunction with the **traceroute** command. For a host to receive SNMP trap notifications for physical topology activity, the **snmp-server enable traps topology** command and the **traceroute** command for that host must be enabled.

Examples

The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to 30 seconds.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology throttle-interval 30
```

The following example shows how to enable SNMP trap notifications for network topology activity and set the throttle timer interval to the default value.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps topology
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
traceroute	Specifies the recipient for SNMP notification messages.
show topology	Displays global physical topology configuration.
topology neighbor cdp	Enables CDP on the interface.

snmp-server host

To specify the recipient for SNMP notification messages, use the **snmp-server host** command. To remove the specified host, use the **no** form of the command.

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

no snmp-server host *host-addr* {**traps** | **informs**}

Syntax Description

host-addr	Specifies the name or IP address of the targeted recipient host.
traps	Sends SNMP trap notifications to this host. This is the default. (Optional)
informs	Sends SNMP inform notifications to this host. (Optional)
version	Specifies the version of the SNMP used to send the traps. (Optional) 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: • **1** —SNMPv1. This option is not available with informs. • **2c** —SNMPv2C. • **3** —SNMPv3. The following three optional keywords can follow the version 3 keyword: – **auth**—Enables MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) packet authentication – **noauth**—Gives the noAuthNoPriv security level. This is the default if no keyword is specified.
community-string	Specifies the password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

udp-port *port*	Specifies the UDP port of the host to use. The range is 0 to 65535. The default is 162. (Optional)
notification-type	Specifies the type of notification to be sent to the host. (Optional) If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: • **alarms**—Sends alarm state change notifications (CISCO-ENTITY-ALARM-MIB). • **aps**—Sends APS MIB (CISCO-APS-MIB) modification notifications. • **bgp**—Sends BGP (Border Gateway Protocol) state change notifications. • **cdl**—Sends in-band message channel MIB (CISCO-CDL-MIB) modification notifications. • **config**—Sends configuration notifications. • **entity**—Sends entity MIB (ENTITY-MIB) modification notifications. • **fru-ctrl**—Sends entity FRU (field replaceable unit) control MIB (CISCO-ENTITY-FRU-CONTROL-MIB) modification notifications. • **oscp**—Sends OSCP MIB (CISCO-OSCP-MIB) modification notifications. • **patch**—Sends optical patch MIB (CISCO-OPTICIAL-PATCH-MIB) modification notifications. • **rf**—Sends redundancy facility MIB (CISCO-RF-MIB) modification notifications. • **snmp**—Sends SNMP notifications (as defined in RFC 1157). • **syslog**—Sends error message notifications (CISCO-SYSLOG-MIB). Specify the level of messages to be sent with the logging history level command. • **threshold**—Sends interface alarm threshold MIB (CISCO-IF-THRESHOLD-MIB) modification notifications. • **topology**—Sends physical topology MIB (PTOPO-MIB) modification notifications. • **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.

Defaults

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

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

If no **version** keyword is present, the default is version 1.

Command Modes

Global configuration

Command History

This table includes the following release-specific history entries:

- EV-Release
- SV-Release
- S-Release

EV-Release	Modification
12.1(10)EV	This command was first introduced.
SV-Release	**Modification**
12.2(18)SV	This command was integrated in this release.
S-Release	**Modification**
12.2(22)S	This command was integrated in this release.

Usage Guidelines

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

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request is held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform might 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. To configure the system 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.

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

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

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

Some notification types cannot be controlled with the **snmp-server enabl**e command. Certain 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.

Examples

The following example shows how to enable SNMP trap notifications for APS activity.

```
Switch# configure terminal
Switch(config)# snmp-server host node1 traps
```

Related Commands

Command	Description
show running-config	Displays the configuration information currently running on the system.
show snmp	Displays the status of SNMP communications.
snmp-server enable traps aps	Enables SNMP trap notification for APS activity.
snmp-server enable traps oscp	Enables SNMP trap notifications for OSCP activity.
snmp-server enable traps patch	Enables SNMP trap notifications for patch connection activity.
snmp-server enable traps rf	Enables SNMP trap notifications for redundancy facility activity.
snmp-server enable traps threshold min-severity	Enables SNMP trap notifications for alarm threshold activity.
snmp-server enable traps topology	Enables SNMP trap notifications for physical topology activity.