



SNMP Commands

This chapter contains the Cisco ONS 15540 ESP-specific SNMP commands. For the complete list of SNMP commands supported on the Cisco ONS 15540 ESP, 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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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 group	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 optical monitor min-severity

To enable SNMP trap notifications defined in optical monitor MIB with the minimum severity threshold, use the **snmp-server enable traps optical monitor min-severity** command. To disable this feature, use the **no** form of the command.

snmp-server enable traps optical monitor min-severity { critical | major | minor | not-alarmed }

no snmp-server enable traps optical monitor min-severity { critical | major | minor | not-alarmed }

Syntax Description		
	critical	Enables trap notifications for critical optical monitor alarms.
	major	Enables trap notifications for major optical monitor alarms.
	minor	Enables trap notifications for minor optical monitor alarms.
	not-alarmed	Enables trap notifications for optical monitor events.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.1(10)EV2	This command was introduced.

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 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 from release 12.2(22)SV.

Usage Guidelines Use this command to enable the SNMP trap notifications defined in the optical monitor MIB (CISCO-OPTICAL-MONITOR-MIB).

The **snmp-server enable traps optical monitor min-severity** 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 optical monitor min-severity** 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 major and critical optical monitor trap activity.

```
Switch# configure terminal  
Switch(config)# snmp-server enable traps optical monitor min-severity major
```

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.
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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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 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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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

<i>host-addr</i>	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	<p>Specifies the version of the SNMP used to send the traps. (Optional)</p> <p>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"> • 1 —SNMPv1. This option is not available with informs. • 2c —SNMPv2C. • 3 —SNMPv3. The following three optional keywords can follow the version 3 keyword: <ul style="list-style-type: none"> – 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.
<i>community-string</i>	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 <i>port</i>	Specifies the UDP port of the host to use. The range is 0 to 65535. The default is 162. (Optional)
<i>notification-type</i>	<p>Specifies the type of notification to be sent to the host. (Optional)</p> <p>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"> • 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. • 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. • optical—Sends optical power modification (CISCO-OPTICAL-MONITOR-MIB) notifications. • oscp—Sends OSCP MIB (CISCO-OSCP-MIB) modification notifications. • patch—Sends optical patch MIB (CISCO-OPTICAL-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:

- EY-Release
- E-Release
- EV-Release
- SV-Release
- S-Release

EY-Release	Modification
12.1(7a)EY2	This command was introduced.
E-Release	Modification
12.1(11b)E	This command was integrated in this release.
EV-Release	Modification
12.1(10)EV	This command was integrated in this release.
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 from release 12.2(22)SV.

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 enable** 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 nodel 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 patch	Enables SNMP trap notification for patch activity.
snmp-server enable traps oscp	Enables SNMP trap notifications for OSCP 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.

■ snmp-server host