OSPF Sham-Link MIB Support

First Published: October 28, 2004
Last Updated: July 13, 2007

This feature introduces MIB support for the OSPF Sham-Link feature through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New commands have been added to enable Simple Network Management Protocol (SNMP) notifications for the Open Shortest Path First (OSPF) sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for OSPF Sham-Link MIB Support" section on page 22.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for OSPF Sham-Link MIB Support

- It is presumed that you already have configured an Open Shortest Path First (OSPF) sham-link.
- SNMP must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.

Restrictions for OSPF Sham-Link MIB Support

All enhancements that are introduced by this feature are provided only by the Cisco private MIBs CISCO-OSPF-MIB and CISCO-OSPF-TRAP-MIB.

Information About OSPF Sham-Link MIB Support

This section contains the following information:

OSPF Sham-Links in PE-PE Router Connections

In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) configuration, a virtual connection called a sham-link can be configured to interconnect between two VPN sites that want to be in the same OSPF area. The sham-link is configured on top of the MPLS VPN tunnel that connects two provider edge (PE) routers. The OSPF packets are propagated over the sham-link. For more information on configuring sham-links, refer the OSPF Sham-Link Support for MPLS VPN feature at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ospfshmk.htm

Cisco OSPF MIB and Cisco OSPF Trap MIB Enhancements

The OSPF Sham-Link MIB Support feature introduces MIB support for OSPF sham-links through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB) for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, 12.2(31)SB2, and 12.2(33)SXH. New CLI has been added to enable SNMP notifications for the OSPF sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface. The following sections describe the enhancements:

OSPF Sham-Link Configuration Support

The cospfShamLinksTable table object stores information about the sham-links that have been configured for the OSPF area. Beginning with Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, 12.2(31)SB2, and 12.2(33)SXH, the cospfShamLinksTable replaces the cospfShamLinkTable. The cospfShamLinksTable allows access to the following MIB objects:

- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksRetransInterval
- cospfShamLinksHelloInterval
- cospfShamLinksRtrDeadInterval
- cospfShamLinksState
- cospfShamLinksEvents
- cospfShamLinksMetric

OSPF Sham-Link Neighbor Support

The cospfShamLinkNbrTable table object describes all OSPF sham-link neighbor entries. The cospfShamLinkNbrTable allows access to the following MIB objects:

- cospfShamLinkNbrArea
- cospfShamLinkNbrIpAddrType
- cospfShamLinkNbrIpAddr
- cospfShamLinkNbrRtrId
- cospfShamLinkNbrOptions
- cospfShamLinkNbrState
- cospfShamLinkNbrEvents
- cospfShamLinkNbrLsRetransQLen
- cospfShamLinkNbrHelloSuppressed

OSPF Sham-Link Interface Transition State Change Support

The cospfShamLinksStateChange trap object is used to notify the network manager of a transition state change for the OSPF sham-link interface. The cospfShamLinksStateChange trap object replaces the original cospfShamLinkStateChange trap object for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2. The cospfShamLinksStateChange trap objects contains the following MIB objects:

- ospfRouterId
- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType

- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksState

OSPF Sham-Link Neighbor Transition State Change Support

The cospfShamLinkNbrStateChange trap object is used to notify the network manager of a transition state change for the OSPF sham-link neighbors. The cospfShamLinkNbrStateChange trap object contains the following MIB objects:

- ospfRouterId
- cospfShamLinkNbrArea
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinkNbrIpAddrType
- cospfShamLinkNbrIpAddr
- cospfShamLinkNbrRtrId
- cospfShamLinkNbrState

Sham-Link Errors

Trap notifications are provided for OSPF sham-link configuration, authentication, and bad packet errors. These errors include the following trap objects:

- cospfShamLinkConfigError
- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

Note The cospfShamLinkAuthFailure trap will not be generated because Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2 do not yet support authentication over sham-links. The cospfShamLinkRxBadPacket trap will not be generated because it also is not supported by Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2. However, the information can be retrieved from the existing OSPF bad packet traps.

How to Configure OSPF Sham-Link MIB Support

This section describes the configuration tasks for the OSPF Sham-Link MIB Support feature. Each task in the list is identified as either required or optional.

- Configuring the Router to Send SNMP Notifications, page 5 (required)
- Enabling OSPF Sham-Link Error Traps, page 6 (required)
- Enabling OSPF Sham-Link Retransmissions Traps, page 7 (required)

- Enabling OSPF Sham-Link State Change Traps, page 8 (required)
- Verifying OSPF Sham-Link MIB Traps on the Router, page 9 (optional)

Configuring the Router to Send SNMP Notifications

Perform this task to enable the router to send SNMP notifications (traps or informs) defined in the OSPF MIBs. SNMP notifications can be configured on the router and GET operations can be performed from an external management station only after MIB support is enabled.

OSPF Configuration Error Notifications

To enable the sending of OSPF configuration errors notifications, enable the following traps:

- cospfShamLinkConfigError
- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
5. **snmp-server enable traps ospf**
6. **end**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show running-config`
	
	Example:
	`Router# show running-config`
		Displays the running configuration to determine if an SNMP agent is already running.
		• If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.

Step 3	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

	Command or Action	Purpose
Step 4	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 172.20.2.162 version 2c public ospf`	Specifies a recipient (target host) for SNMP notification operations. • If no *notification-type* is specified, all enabled notifications (traps or informs) will be sent to the specified host. • If you want to send only the OSPF notifications to the specified host, you can use the optional **ospf** keyword as one of the *notification-types*. (See the example.)
Step 5	**snmp-server enable traps ospf** **Example:** `Router(config)# snmp-server enable traps ospf`	Enables all SNMP notifications defined in the OSPF MIBs. **Note** This step is required only if you wish to enable all OSPF traps, including the traps for OSPF sham-links. When you enter the **no snmp-server enable traps ospf** command, all OSPF traps, including the OSPF sham-link trap, will be disabled.
Step 6	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

Enabling OSPF Sham-Link Error Traps

Notifications are sent when OSPF sham-link configuration errors are detected. To enable the sending of sham-link configuration error notifications, enable the following cospfShamLinkConfigError trap.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ospf cisco-specific errors config-error**
4. **snmp-server enable traps ospf cisco-specific errors shamlink** [**authentication** [**bad-packet** [**config**] | [**config** [**bad-packet**]]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps ospf cisco-specific errors config-error** **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific errors config-error`	Enables error traps for OSPF nonvirtual interface mismatch errors. **Note** You must enter the **snmp-server enable traps ospf cisco-specific errors config-error** command before you enter the **snmp-server enable traps ospf cisco-specific errors shamlink** command, in order for both traps to be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links. If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.
Step 4	**snmp-server enable traps ospf cisco-specific errors shamlink** [**authentication** [**bad-packet** [**config**] | [**config** [**bad-packet**]]] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink`	Enables error traps for OSPF sham-link errors. • The **authentication** keyword enables SNMP notifications only for authentication failures on OSPF sham-link interfaces. • The **bad-packet** keyword enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces. • The **config** keyword enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.
Step 5	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

Enabling OSPF Sham-Link Retransmissions Traps

Notifications are sent when OSPF packets retransmissions across a sham-link are detected. To enable the sending of sham-link packet retransmission notifications, enable the following cospfShamLinkTxRetransmit trap.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ospf cisco-specific retransmit** [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps ospf cisco-specific retransmit** [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink`	Enables error traps for OSPF sham-link retransmission errors.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

Enabling OSPF Sham-Link State Change Traps

Notifications are sent when sham-link interface and neighbor state changes are detected. To enable the sending of sham-link state changes notifications, you can enable the following cospfShamLinksStateChange trap, which replaces the original cospfShamLinkStateChange trap, as well as the cospfShamLinkNbrStateChange trap, which is new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2:

- cospfShamLinksStateChange
- cospfShamLinkNbrStateChange

Note The replaced cospfShamLinkChange trap can still be enabled, but not when you want to enable the new cospfShamLinksStateChange trap.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change** | **shamlink** [**interface** | **interface-old** | **neighbor**]] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific state-change`	Enables all Cisco-specific OSPF state change traps including the cospfShamLinksStateChange and cospfShamLinkNbrStateChange traps that are new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2. • The **neighbor** keyword enables the OSPF sham-link neighbor state change traps. • The **interface** keyword enables the OSPF sham-link interface state change traps. • The **interface-old** keyword enables the original OSPF sham-link interface state change trap that is replaced by the cospfShamLinksStateChange and cospfShamLinkNbrStateChange traps for Cisco IOS Releases 12.0(30)S and 12.3(14)T. **Note** You cannot enter both the **interface** and **interface-old** keywords because you cannot enable both the new and replaced sham-link interface transition state change traps. You can configure only one of the two traps, but not both.
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

Verifying OSPF Sham-Link MIB Traps on the Router

This task verifies that you have enabled OSPF sham-link MIB support.

SUMMARY STEPS

1. **enable**
2. **show running-config | include traps**

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show running-config | include traps`
	
	Example:
	`Router# show running-config | include traps`
		Displays the contents of the currently running configuration file and includes information about enabled traps.
		• Verifies if the trap is enabled.

Configuration Examples for OSPF Sham-Link MIB Support

This section provides the following configuration examples:

- Enabling and Verifying OSPF Sham-Link Error Traps: Example, page 10
- Enabling and Verifying OSPF State Change Traps: Example, page 11
- Enabling and Verifying OSPF Sham-Link Retransmissions Traps: Example, page 12

Enabling and Verifying OSPF Sham-Link Error Traps: Example

The following example enables all Cisco-specific OSPF sham-link error traps. Note that the first attempt to enter the **snmp-server enable traps ospf cisco-specific errors shamlink** command results in an error message that the **snmp-server enable traps ospf cisco-specific errors config-error** command must be entered first:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
% Sham-link config error trap not enabled.
% Configure "cisco-specific errors config-error" first.
% This requirement allows both traps to be sent.
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# end
```

The **show running-config** command is entered to verify that the traps are enabled:

```
Router# show running-config | include traps

snmp-server enable traps ospf cisco-specific errors config-error
snmp-server enable traps ospf cisco-specific errors shamlink
```

At the time of disabling the traps, if the **no snmp-server enable traps ospf cisco-specific errors config-error** command is entered before the **snmp-server enable traps ospf cisco-specific errors shamlink** command, a message will be displayed to indicate that the sham-link configuration errors traps have also been disabled:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# no snmp-server enable traps ospf cisco-specific errors config-error
! This command also disables the previously-enabled shamlink configuration error traps.
Router(config)# end
```

Enabling and Verifying OSPF State Change Traps: Example

The following example enables all Cisco-specific OSPF state change traps including the cospfShamLinksStateChange and cospfShamLinkNbrStateChange traps that are new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
```

The **show running-config** command is entered to verify that the traps are enabled:

```
Router# show running-config | include traps

snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
```

Note that the **snmp-server enable traps ospf cisco-specific state-change shamlink** command enables the sham-link interface state change for the cospfShamLinksStateChange trap that is new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2.

To enable the original cospfShamLinkStateChange trap, you must first disable the cospfShamLinksStateChange trap. An attempt to enter the **snmp-server enable traps ospf cisco-specific state-change shamlink interface-old** command results in the following error message:

```
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old
% Cannot enable both sham-link state-change interface traps.
% Deprecated sham link interface trap not enabled.
Router(config)# no snmp-server enable traps ospf cisco-specific state-change shamlink
interface
Router(config)# snmp-server enable traps ospf cisco-specific state-change shamlink
interface-old
```

Enabling and Verifying OSPF Sham-Link Retransmissions Traps: Example

The following example enables all OSPF sham-link retransmissions traps:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
Router(config)# end
```

The **show running-config** command is entered to verify that the traps are enabled:

```
Router# show running-config | include traps

snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" part of the *Cisco IOS Network Management Configuration Guide*, Release 12.4T.

Additional References

The following sections provide references related to the OSPF Sham-Link MIB Support feature.

Related Documents

Related Topic	Document Title
Configuring OSPF sham-links	*OSPF Sham-Link Support for MPLS VPN*
SNMP configuration	*Cisco IOS Network Management Configuration Guide*, Release 12.4T
SNMP commands	*Cisco IOS Network Management Command Reference*, Release 12.4T *Cisco IOS Network Management Command Reference*, Release 12.2SB *Cisco IOS Network Management Command Reference*, Release 12.2SR

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
• CISCO-OSPF-MIB • CISCO-OSPF-TRAP-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **snmp-server enable traps ospf cisco-specific errors config-error**
- **snmp-server enable traps ospf cisco-specific errors shamlink**
- **snmp-server enable traps ospf cisco-specific retransmit**
- **snmp-server enable traps ospf cisco-specific state-change**

snmp-server enable traps ospf cisco-specific errors config-error

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) nonvirtual interface mismatch errors, use the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. To disable OSPF nonvirtual interface mismatch error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific errors config-error

no snmp-server enable traps ospf cisco-specific errors config-error

Syntax Description

This command has no keywords or arguments.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF nonvirtual interface mismatch errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.3(5)	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

The following example enables the router to send nonvirtual interface mismatch error notifications to the host at the address myhost.cisco.com using the community string defined as public:

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

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors shamlink	Enables SNMP notifications for OSPF sham-link errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific errors shamlink

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

snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]]

no snmp-server enable traps ospf cisco-specific errors shamlink [**authentication** [**bad-packet**] [[**config**] | **config** [**bad-packet**]]]]

Syntax Description

authentication	(Optional) Enables SNMP notifications only for authentication failures on OSPF sham-link interfaces.
bad-packet	(Optional) Enables SNMP notifications only for packet parsing failures on OSPF sham-link interfaces.
config	(Optional) Enables SNMP notifications only for configuration mismatch errors on OSPF sham-link interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF sham-link errors are not created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

To enable the cospfShamLinkConfigError trap, you must first enter the **snmp-server enable traps ospf cisco-specific errors config-error** command in global configuration mode. The **snmp-server enable traps ospf cisco-specific errors config-error** command enables the cospfConfigError trap, so that both traps can be generated at the same place and maintain consistency with a similar case for configuration errors across virtual links.

If you try to enable the cospfShamLinkConfigError trap before configuring the cospfospfConfigError trap you will receive an error message stating you must first configure the cospfConfigError trap.

Examples

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

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

Related Commands

Command	Description
snmp-server enable traps ospf cisco-specific errors config-error	Enables SNMP notifications for OSPF nonvirtual interface mismatch errors.
snmp-server enable traps ospf cisco-specific retransmit	Enables SNMP notifications for OSPF retransmission errors.
snmp-server enable traps ospf cisco-specific state-change	Enables SNMP notifications for OSPF transition state changes.

snmp-server enable traps ospf cisco-specific retransmit

To enable Simple Network Management Protocol (SNMP) notifications for Open Shortest Path First (OSPF) retransmission errors, use the **snmp-server enable traps ospf cisco-specific retransmit** command in global configuration mode. To disable OSPF sham-link error SNMP notifications, use the **no** form of this command.

snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

no snmp-server enable traps ospf cisco-specific retransmit [**packets** [**shamlink** | **virt-packets**] | **shamlink** [**packets** | **virt-packets**] | **virt-packets** [**shamlink**]]

Syntax Description

packets	(Optional) Enables SNMP notifications only for packet retransmissions on nonvirtual interfaces.
shamlink	(Optional) Enables SNMP notifications only for sham-link retransmission notifications.
virt-packets	(Optional) Enables SNMP notifications only for packet retransmissions on virtual interfaces.

Command Default

This command is disabled by default; therefore, SNMP notifications for OSPF retransmission errors are not created.

Command Modes

Global configuration

Command History

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

Examples

The following example enables the router to send OSPF sham-link retransmission notifications:

```
Router(config)# snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Related Commands

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

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

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

Feature Information for OSPF Sham-Link MIB Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for OSPF Sham-Link MIB Support

Feature Name	Releases	Feature Information
OSPF Sham-Link MIB Support	12.0(30)S 12.3(14)T 12.2(33)SRA 12.2(31)SB2 12.2(33)SXH	This feature introduces MIB support for the OSPF Sham-Link feature through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New commands have been added to enable Simple Network Management Protocol (SNMP) notifications for the Open Shortest Path First (OSPF) sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface.