OSPF Sham-Link MIB Support

Last Updated: November 1, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for OSPF Sham-Link MIB Support

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

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

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

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 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, see the " OSPF Sham-Link Support for MPLS VPN" chapter.

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). New command-line interface (CLI) commands have 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.

OSPF Sham-Link Configuration Support

The cospfShamLinksTable table object stores information about the sham-links that have been configured for the OSPF area. 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 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

How to Configure OSPF Sham-Link MIB Support

Configuring the Router to Enable Sending of SNMP Notifications

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.

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
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 want 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 Sending of OSPF Sham-Link Error Traps

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

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

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. • 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. **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.

	Command or Action	Purpose
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

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

Example Enabling and Verifying OSPF Sham-Link Error Traps

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
```

Example Enabling and Verifying OSPF State Change Traps

The following example enables all Cisco-specific OSPF state change traps including the cospfShamLinksStateChange and cospfShamLinkNbrStateChange traps:

```
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.

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
```

Example Enabling and Verifying OSPF Sham-Link Retransmissions Traps

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 XE Network Management Configuration Guide, Release 2* .

Additional References

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF sham-links	OSPF Sham-Link Support for MPLS VPN
SNMP configuration	"Configuring SNMP Support"
SNMP commands	*Cisco IOS Network Management Command Reference*
Configuring OSPF	Configuring OSPF
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for OSPF Sham-Link MIB Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for OSPF Sham-Link MIB Support

Feature Name	Releases	Feature Information
OSPF Sham-Link MIB Support	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	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 to 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. The following commands are introduced or modified in the feature documented in this module: • **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.**