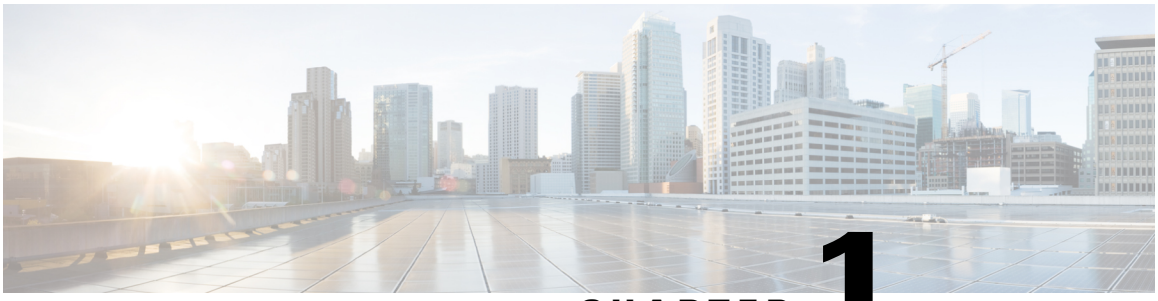
IP Routing: OSPF Configuration Guide, Cisco IOS XE Release 3E

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

This module describes configuration tasks to configure various options involving Open Shortest Path First (OSPF). This module contains tasks that use commands to configure a lightweight security mechanism to protect OSPF sessions from CPU-utilization-based attacks and to configure a router to shut down a protocol temporarily without losing the protocol configuration.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

Information About OSPF TTL Security Check and OSPF Graceful Shutdown

TTL Security Check for OSPF

When the TTL Security Check feature is enabled, OSPF sends outgoing packets with an IP header Time to Live (TTL) value of 255 and discards incoming packets that have TTL values less than a configurable threshold. Since each device that forwards an IP packet decrements the TTL, packets received via a direct (one-hop) connection will have a value of 255. Packets that cross two hops will have a value of 254, and so on. The receive threshold is configured in terms of the maximum number of hops that a packet may have traveled. The value for this *hop-count* argument is a number from 1 to 254, with a default of 1.

The TTL Security Check feature may be configured under the OSPF router submode, in which case it applies to all the interfaces on which OSPF runs, or it may be configured on a per-interface basis.

Transitioning Existing Networks to Use TTL Security Check

If you currently have OSPF running in your network and want to implement TTL security on an interface-by-interface basis without any network interruptions, use the **ip ospf ttl-security** command and set the hop-count argument to 254. This setting causes outgoing packets to be sent with a TTL value of 255, but allows any value for input packets. Later, once the device at the other end of the link has had TTL security enabled you can start enforcing the hop limit for the incoming packets by using the same **ip ospf ttl-security** command with no hop count specified. This process ensures that OSPF packets will not be dropped because of a temporary mismatch in TTL security.

TTL Security Check for OSPF Virtual and Sham Links

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a *virtual link*. The virtual link must be configured in both devices. The configuration information in each device consists of the other virtual endpoint (the other area border router [ABR]) and the nonbackbone area that the two devices have in common (called the *transit area*.) Note that virtual links cannot be configured through stub areas. Sham links are similar to virtual links in many ways, but sham links are used in Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) networks to connect Provider Edge (PE) routers across the MPLS backbone.

To establish a virtual link or a sham link, use the **area virtual-link** or **area sham-link cost** commands, respectively, in router configuration mode. To configure the TTL Security Check feature on a virtual link or a sham link, configure the **ttl-security** keyword and the *hop-count* argument in either command. Note that the *hop-count* argument value is mandatory in this case.

Benefits of the OSPF Support for TTL Security Check

The OSPF Support for TTL Security Check feature provides an effective and easy-to-deploy solution to protect OSPF neighbor sessions from CPU utilization-based attacks. When this feature is enabled, a host cannot attack an OSPF session if the host is not a member of the local or remote OSPF network, or if the host is not directly

connected to a network segment between the local and remote OSPF networks. This solution greatly reduces the effectiveness of Denial of Service (DoS) attacks against an OSPF autonomous system.

OSPF Graceful Shutdown

The OSPF Graceful Shutdown feature provides the ability to temporarily shut down the OSPF protocol in the least disruptive manner and notify its neighbors that it is going away. All traffic that has another path through the network will be directed to that alternate path. A graceful shutdown of the OSPF protocol can be initiated using the **shutdown** command in router configuration mode.

This feature also provides the ability to shut down OSPF on a specific interface. In this case, OSPF will not advertise the interface or form adjacencies over it; however, all of the OSPF interface configuration will be retained. To initiate a graceful shutdown of an interface, use the **ip ospf shutdown** command in interface configuration mode.

How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown

Configuring TTL Security Check on All OSPF Interfaces

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **ttl security all-interfaces** [**hops** *hop-count*]
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.

	Command or Action	Purpose
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 109`	Enables OSPF routing, which places the device in router configuration mode.
Step 4	**ttl security all-interfaces** [**hops** *hop-count*] **Example:** `Router(config-router)# ttl security all-interfaces`	Configures TTL security check on all OSPF interfaces. **Note** This configuration step applies only to normal OSPF interfaces. This step does not apply to virtual links or sham links that require TTL security protection. Virtual links and sham links must be configured independently.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

Configuring TTL Security Check on a Per-Interface Basis

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf ttl-security** [**hops** *hop-count* | **disable**]
5. **end**
6. **show ip ospf** [*process-id*] **interface** [*interface type interface-number*] [**brief**] [**multicast**] [**topology** *topology-name* | **base**}]
7. **show ip ospf neighbor** *interface-type interface-number* [*neighbor-id*][**detail**]
8. **show ip ospf** [*process-id*] **traffic** [*interface-type interface-number*]
9. **debug ip ospf adj**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf ttl-security** [**hops** *hop-count* | **disable**] **Example:** `Router(config-if)# ip ospf ttl-security`	Configures TTL security check feature on a specific interface. • The *hop-count*argument range is from 1 to 254. • The **disable** keyword can be used to disable TTL security on an interface. It is useful only if the **ttl-security all-interfaces** comand initially enabled TTL security on all OSPF interfaces, in which case **disable** can be used as an override or to turn off TTL security on a specific interface. • In the example, TTL security is being disabled on GigabitEthernet interface 0/0/0.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf** [*process-id*] **interface** [*interface type interface-number*] [**brief**] [**multicast**] [**topology** *topology-name* | **base**}] **Example:** `Router# show ip ospf interface gigabitethernet 0/0/0`	(Optional) Displays OSPF-related interface information.
Step 7	**show ip ospf neighbor** *interface-type interface-number* [*neighbor-id*][**detail**] **Example:** `Router# show ip ospf neighbor 10.199.199.137`	(Optional) Displays OSPF neighbor information on a per-interface basis. • If one side of the connection has TTL security enabled, the other side shows the neighbor in the INIT state.

	Command or Action	Purpose
Step 8	**show ip ospf** [*process-id*] **traffic** [*interface-type interface-number*] **Example:** `Router# show ip ospf traffic`	(Optional) Displays OSPF traffic statistics. • The number of times a TTL security check failed is included in the output.
Step 9	**debug ip ospf adj** **Example:** `Router# debug ip ospf adj`	(Optional) Initiates debugging of OSPF adjacency events. • Information about dropped packets, including interface type and number, neighbor IP address, and TTL value, is included in the command output.

Configuring OSPF Graceful Shutdown on a Per-Interface Basis

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf shutdown**
5. **end**
6. **show ip ospf [** *process-id* **] interface [** *interface type interface-number]* **[brief** *]* [**multicast**] [**topology** *topology-name* | **base**}]
7. **show ip ospf [** *process-id* **]**

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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)#` **interface GigabitEthernet 0/1/0**	Configures an interface type and number and enters interface configuration mode.
Step 4	**ip ospf shutdown** **Example:** `Router(config-if)#` **ip ospf shutdown**	Initiates an OSPF protocol graceful shutdown at the interface level. • When the **ip ospf shutdown** interface command is entered, the interface on which it is configured sends a link-state update advising its neighbors that is going down, which allows those neighbors to begin routing OSPF traffic around this router.
Step 5	**end** **Example:** `Router(config-if)#` **end**	Returns to privileged EXEC mode.
Step 6	**show ip ospf [** *process-id* **] interface [** *interface type interface-number* **]** [**brief**] [**multicast**] [**topology** *topology-name* | **base**}] **Example:** `Router#` **show ip ospf interface GigabitEthernet 0/1/0**	(Optional) Displays OSPF-related interface information.
Step 7	**show ip ospf [** *process-id* **]** **Example:** `Router#` **show ip ospf**	(Optional) Displays general information about OSPF routing processes.

Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

Example: Transitioning an Existing Network to Use TTL Security Check

The following example shows how to enable TTL security in an existing OSPF network on a per-interface basis.

Configuring TTL security in an existing network is a three-step process:

1. Configure TTL security with a hop count of 254 on the OSPF interface on the sending side device.
2. Configure TTL security with no hop count on the OSPF interface on the receiving side device.
3. Reconfigure the sending side OSPF interface with no hop count.

```
configure terminal
 ! Configure the following command on the sending side router.
 interface gigabitethernet 0/1/0
  ip ospf ttl-security hops 254
 ! Configure the next command on the receiving side router.
 interface gigabitethernet 0/1/0
  ip ospf ttl-security
 ! Reconfigure the sending side with no hop count.
  ip ospf ttl-security
  end
```

Additional References

The following sections provide references related to the OSPF TTL Security Check and OSPF Graceful Shutdown features.

Related Documents

Related Topic	Document Title
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 and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, 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 and support for existing RFCs has not been modified.	--

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

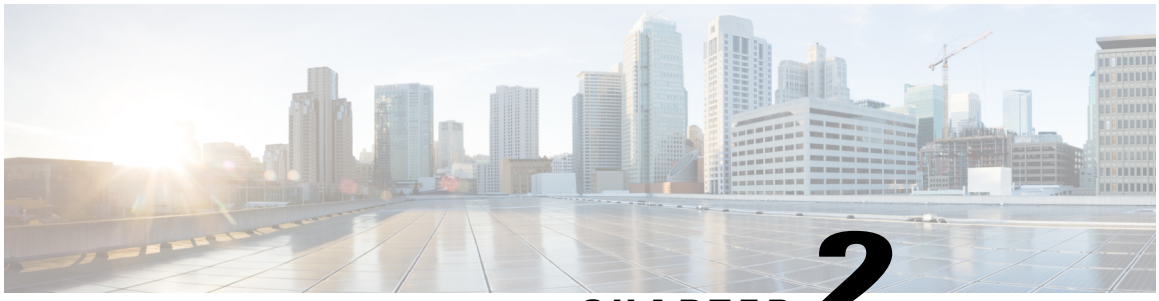
Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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 Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

Feature Name	Releases	Feature Information
OSPF Graceful Shutdown	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SG Cisco IOS Release 15.1(1)SG	This feature provides the ability to temporarily shut down a protocol in the least disruptive manner and to notify its neighbors that it is going away. A graceful shutdown of a protocol can be initiated on all OSPF interfaces or on a specific interface. The following commands were introduced or modified: • **ip ospf shutdown** • **show ip ospf** • **show ip ospf interface** • **shutdown (router OSPF)**
OSPF TTL Security Check	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SG Cisco IOS Release 15.1(1)SG	This feature increases protection against OSPF denial of service attacks, enables checking of TTL values on OSPF packets from neighbors, and allows users to set TTL values sent to neighbors. The following commands were introduced or modified: • **area sham-link cost** • **area virtual-link** • **debug ip ospf adj** • **ip ospf ttl-security** • **show ip ospf interface** • **show ip ospf neighbor** • **show ip ospf traffic** • **ttl-security all-interfaces**



CHAPTER 2

Enabling OSPFv2 on an Interface Basis

This document describes how to enable Open Shortest Path First version 2 (OSPFv2) on a per-interface basis to simplify the configuration of unnumbered interfaces. The **ip ospf area** command allows you to enable OSPFv2 explicitly on an interface. The **ip ospf area** command is an alternative to enabling OSPFv2 through the address of the interface that matches the address range specified by the **network area** command.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Enabling OSPFv2 on an Interface Basis

OSPFv2 must be running on your network.

Restrictions on Enabling OSPFv2 on an Interface Basis

The **ip ospf area** command is supported only for OSPFv2.

Information About Enabling OSPFv2 on an Interface Basis

Benefits of Enabling OSPFv2 on an Interface Basis

OSPF is enabled on an interface when the network address for the interface matches the range of addresses that is specified by the **network area** command, which is entered in router configuration mode. Alternatively, you can enable OSPFv2 explicitly on an interface by using the **ip ospf area** command, which is entered in interface configuration mode. This capability simplifies the configuration of unnumbered interfaces with different areas.

Because the **ip ospf area** command is configured explicitly for an interface, it supersedes the effects of the **network area**command, which is entered at the network level to affect the interfaces whose addresses fall within the address range specified for the **network area** command.

If you later disable the **ip ospf area** command, the interface still will run OSPFv2 as long as its network address matches the range of addresses that is specified by the **network area**command.

Implications of Configuring OSPFv2 On a Router Basis or an Interface Basis

Before you use the **ip ospf area** command to enable OSPFv2 on an interface, we recommend that you understand the following scenarios and command behavior. There are implications to using the **network area**command (configuring OSPFv2 in router configuration mode) versus using the **ip ospf area** command (configuring OSPFv2 in interface configuration mode).

Interface Is Already OSPFv2-Enabled by network area Command with Same Area and Process

If you enter the **ip ospf area** command on an interface that is enabled in OSPFv2 by the **network area**command, the process ID or area ID of the interface does not change, and the interface status will not be changed. However, the interface will be flagged as being configured from interface configuration mode, and the configuration data will be saved in the interface description block (IDB).

Interface Is Already Configured by network area Command with Different Area or Process

If you enter the **ip ospf area** command on an interface that is enabled in OSPFv2 by the **network area**command, but you change the configuration by changing the process ID and area ID of the interface, after the new configuration information is stored in the IDB, the interface will be removed and reattached. Therefore, the interface will be removed from the original area and process and be added to the new ones. The state of the interface will also be reset.

Interface Is Not Configured by network area Command

If the interface is not enabled in OSPFv2 by the **network area** command, the area and OSPF router instance will be created if needed. When the router is reloaded, the OSPF process will not begin running until system

initialization is complete. To remove an OSPF router instance, enter the **no router ospf** command. Removing the **ip ospf area** command in interface mode will not result in removing an OSPF router instance.

Removing an ip ospf area Command

When the **ip ospf area**command is removed, the interface will be detached from the area. The area will be removed if it has no other attached interfaces. If the interface address is covered by the **network area** command, the interface will be enabled once again in the area for the network that it is in.

New Processes

If an OSPF process does not already exist, and a router ID cannot be chosen when either the **router ospf** command or the **interface** command is configured, a Proximity Database (PDB) and a process will be created, but the process will be inactive. The process will become active when a router ID is chosen, either when it is explicitly configured using the **router-id** command or when an IP address becomes available. Note that the **router ospf** command will now be accepted even if a router ID cannot be chosen, putting the command-line interface (CLI) into the OSPF configuration context. Therefore, the **router-id** command is to be entered before an IP address is available. If the process is not active and the **show ip ospf**command is entered, the message "%OSPF: Router process X is not running, please provide a router-id" will be displayed.

Link-State Advertisements and Shortest Path First

If a state change occurs as a result of the **ip ospf area**command, new router link-state advertisements (LSAs) will be generated (also for the old area, if the interface is changing areas) and shortest path first (SPF) will be scheduled to run in both the old and new areas.

How to Enable OSPFv2 on an Interface Basis

Enabling OSPFv2 on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf** *process-id* **area** *area-id* [**secondaries none**]
5. **end**
6. **show ip ospf interface** [*type -number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface FastEthernet 0/2/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf** *process-id* **area** *area-id* [**secondaries none**] **Example:** `Router(config-if)# ip ospf 1 area 0 secondaries none`	Enables OSPFv2 on an interface. • To prevent secondary IP addresses on the interface from being advertised, you must enter the optional **secondaries** keyword followed by the **none** keyword.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show ip ospf interface** [*type -number*] **Example:** `Router# show ip ospf interface FastEthernet 0/2/1`	Displays OSPF-related interface information. • Once you have enabled OSPFv2 on the interface, you can enter the **show ip ospf interface**command to verify the configuration.

Configuration Example for Enabling OSPFv2 on an Interface

Example Enabling OSPFv2 on an Interface

In the following example, OSPFv2 is configured explicitly on GigabitEthernet interface 0/0/0:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# bandwidth 10000
Router(config-if)# ip address 172.16.1.1 255.255.255.0
```

```
Router(config-if)# ip ospf hello-interval 1
Router(config-if)# ip ospf 1 area 0
```

When the **show ip ospf interface** command is entered, the following output shows that GigabitEthernet interface 0/0/0 was configured in interface configuration mode to run OSPFv2. The secondary IP addresses on the interface will also be advertised:

```
Router# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0
  Process ID 1, Router ID 172.16.11.11, Network Type BROADCAST, Cost: 10
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.11.11, Interface address 172.16.1.1
  Backup Designated router (ID) 172.16.22.11, Interface address 172.16.1.2
  Timer intervals configured, Hello 1, Dead 4, Wait 4, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.26.22.11  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Additional References

The following sections provide references related to enabling OSPFv2 on an interface.

Related Documents

Related Topic	Document Title
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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2328	*OSPF Version 2*

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

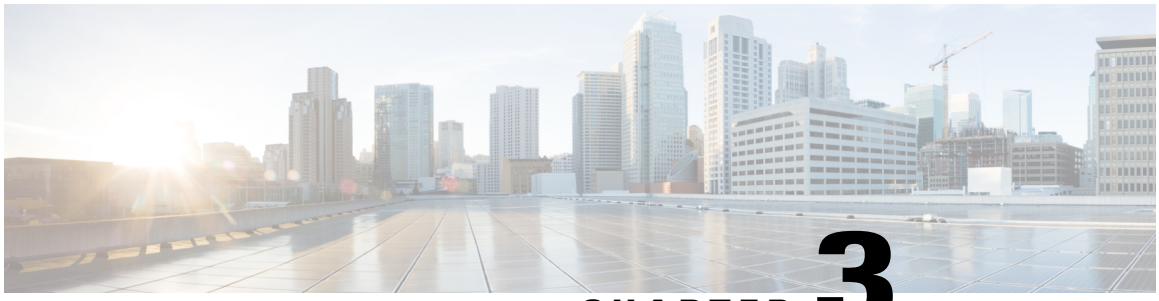
Feature Information for Enabling OSPFv2 on an Interface Basis

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 2: Feature Information for Enabling OSPFv2 on an Interface Basis

Feature Name	Releases	Feature Information
Enabling OSPFv2 on an Interface Basis **Note** This feature was originally named "Area Command in Interface Mode for OSPFv2."	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SG Cisco IOS Release 15.1(1)SG	This document describes how to enable OSPFv2 on a per-interface basis to simplify the configuration of unnumbered interfaces. The **ip ospf area** command allows you to enable OSPFv2 explicitly on an interface. The **ip ospf area** command is an alternative to enabling OSPFv2 through the address of the interface that matches the address range specified by the **network area** command. The following commands are introduced or modified in the feature documented in this module: • **ip ospf area.**



CHAPTER 3

OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

This document describes new and modified commands that provide enhanced OSPF traffic statistics for OSPFv2 and OSPFv3. The ability to collect and display more detailed traffic statistics increases high availability for the OSPF network by making the troubleshooting process more efficient.

New OSPF traffic statistics are collected and displayed to include the following information:

- OSPF Hello input queue and OSPF process queue status and statistics.
- Global OSPF traffic statistics.
- Per OSPF interface traffic statistics.
- Per OSPF process traffic statistics.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Enhanced Traffic Statistics

OSPFv2 or OSPFv3 must be configured on the router.

Information About OSPF Enhanced Traffic Statistics

The OSPF enhanced traffic statistics are enabled by default and cannot be disabled. The detailed OSPF traffic statistics are especially beneficial for troubleshooting the following types of OSPF instabilities:

- OSPF process queue status and statistical information can help the network administrator determine if an OSPF process can handle the amount of traffic sent to OSPF.
- OSPF packet header errors and LSA errors statistics keep a record of different errors found in received OSPF packets.

OSPF enhanced traffic control statistics also monitor the amount of traffic control exchanged between OSPF processes--an important consideration in network environments with slow links and frequent topology changes.

How to Display and Clear OSPF Enhanced Traffic Statistics

Displaying and Clearing OSPF Traffic Statistics for OSPFv2

Before You Begin

Your network must run IPv4 to collect, display and clear detailed traffic statistics for Hello output, process queue status, global OSPF traffic statistics, per OSPF interface traffic statistics and per OSPF process traffic statistics.

SUMMARY STEPS

1. **enable**
2. **show ip ospf** [*process-id*] **traffic**[*interface-type interface-number*]
3. **clear ip ospf traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ip ospf traffic statistics`	Displays OSPFv2 traffic statistics.
Step 3	**clear ip ospf traffic** **Example:** `Router# clear ip ospf traffic`	Clears OSPFv2 traffic statistics.

Displaying and Clearing OSPF Traffic Statistics for OSPFv3

Before You Begin

Your network must run IPv6 to collect, display and clear detailed traffic statistics for Hello output, process queue status, global OSPF traffic statistics, per OSPF interface traffic statistics and per OSPF process traffic statistics.

SUMMARY STEPS

1. **enable**
2. **show ipv6 ospf** [*process-id*] **traffic**[*interface-type interface-number*]
3. **clear ipv6 ospf traffic**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ipv6 ospf traffic statistics`	Displays OSPFv3 traffic statistics.

	Command or Action	Purpose
Step 3	**clear ipv6 ospf traffic** **Example:** `Router# clear ipv6 ospf traffic`	Clears OSPFv3 traffic statistics.

Configuration Examples for OSPF Enhanced Traffic Commands

Displaying and Clearing Enhanced Traffic Statistics for OSPFv2 Example

The following example shows display output for the **show ip ospf traffic** command for OSPFv2:

```
Router# show ip ospf traffic
OSPF statistics:
 Rcvd: 55 total, 0 checksum errors
       22 hello, 7 database desc, 2 link state req
       6 link state updates, 6 link state acks
  Sent: 68 total
       45 hello, 7 database desc, 2 link state req
       10 link state updates, 4 link state acks
           OSPF Router with ID (10.1.1.1) (Process ID 8)
OSPF queues statistic for process ID 8:
  OSPF Hello queue size 0, no limit, drops 0, max size 0
  OSPF Router queue size 0, limit 200, drops 0, max size 0
Interface statistics:
    Interface Ethernet0/0.1
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0
  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 8:
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
```

```
  RX LS req     0                   0
  RX LS upd     0                   0
  RX LS ack     0                   0
  RX Total      0                   0
  TX Failed     0                   0
  TX Hello      16                  1216
  TX DB des     0                   0
  TX LS req     0                   0
  TX LS upd     0                   0
  TX LS ack     0                   0
  TX Total      16                  1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
           OSPF Router with ID (10.1.1.4) (Process ID 1)
OSPF queues statistic for process ID 1:
  OSPF Hello queue size 0, no limit, drops 0, max size 2
  OSPF Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
OSPF packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      11                  528
  RX DB des     4                   148
  RX LS req     1                   60
  RX LS upd     3                   216
  RX LS ack     2                   128
  RX Total      21                  1080
  TX Failed     0                   0
 TX Hello      14                  1104
  TX DB des     3                   252
  TX LS req     1                   56
  TX LS upd     3                   392
  TX LS ack     2                   128
  TX Total      23                  1932
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPF packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      13                  620
  RX DB des     3                   116
  RX LS req     1                   36
  RX LS upd     3                   228
  RX LS ack     4                   216
  RX Total      24                  1216
  TX Failed     0                   0
  TX Hello      17                  1344
  TX DB des     4                   276
  TX LS req     1                   56
  TX LS upd     7                   656
  TX LS ack     2                   128
  TX Total      31                  2460
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
```

```
  Type 0, Length 0, Data 0, Checksum 0,

Summary traffic statistics for process ID 1:
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      24                   1148
  RX DB des     7                    264
  RX LS req     2                    96
  RX LS upd     6                    444
  RX LS ack     6                    344
  RX Total      45                   2296
  TX Failed     0                    0
  TX Hello      31                   2448
  TX DB des     7                    528
  TX LS req     2                    112
  TX LS upd     10                   1048
  TX LS ack     4                    256
  TX Total      54                   4392
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The network administrator can issue the **clear ip ospf traffic** command to reset all counters and restart all statistics collections:

```
Router# clear ip ospf traffic
```

Displaying and Clearing Enhanced Traffic Statistics for OSPFv3 Example

The following example shows display output for the **show ipv6 ospf traffic** command for OSPFv3:

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
            OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852
  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
```

```
  TX Total      18                  900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface Ethernet0/0
OSPFv3 packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      6                   240
  RX DB des     3                   144
  RX LS req     1                   52
  RX LS upd     5                   372
  RX LS ack     2                   152
  RX Total      17                  960
  TX Failed     0                   0
  TX Hello      11                  420
  TX DB des     9                   312
  TX LS req     1                   52
  TX LS upd     5                   376
  TX LS ack     3                   148
  TX Total      29                  1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      11                  436
  RX DB des     7                   316
  RX LS req     2                   104
  RX LS upd     9                   692
  RX LS ack     4                   264
  RX Total      33                  1812
  TX Failed     0                   0
  TX Hello      19                  724
  TX DB des     12                  456
  TX LS req     2                   104
  TX LS upd     8                   628
  TX LS ack     6                   296
  TX Total      47                  2208
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

The network administrator can issue the **clear ipv6 ospf traffic** command to reset all counters and restart all statistics collections:

```
Router# clear ipv6 ospf traffic
```

Additional References

The following sections provide references related to the OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3 feature.

Related Documents

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
OSPF configuration	Configuring OSPF

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	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
	--

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

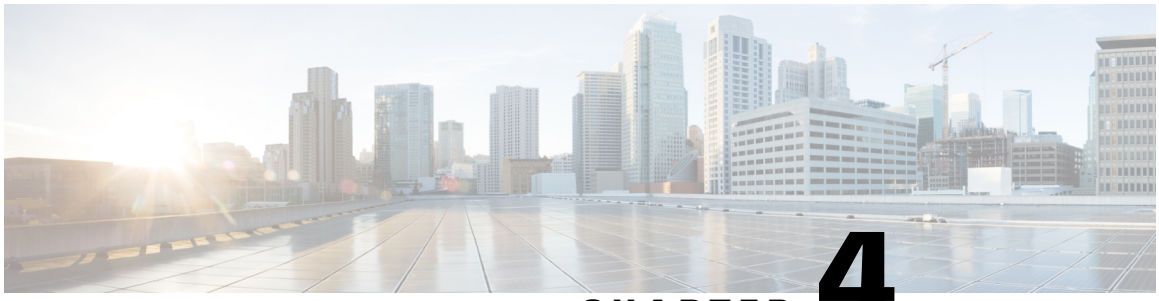
Feature Information for OSPF Enhanced Traffic Statistics

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 3: Feature Information for OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

Feature Name	Releases	Feature Information
OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3	Cisco IOS Release 12.4(6)T Cisco IOS Release 12.2(31)SB2 Cisco IOS Release 12.2(33)SRB Cisco IOS Release 15.1(1)SG Cisco IOS XE Release 3.3SG	This document describes the detailed OSPF traffic statistics that are provided when the user enters the new and modified commands show commands for OSPFv2 and OSPFv3. The following commands were introduced or modified: **clear ipv6 ospf traffic**, **show ip ospf traffic**, **show ipv6 ospf traffic**.



CHAPTER 4

OSPF SNMP ifIndex Value for Interface ID in Data Fields

This feature allows you to configure the interface ID value Open Shortest Path First version 2 (OSPFv2) and Open Shortest Path First version 3 (OSPFv3) data fields. You can choose to use either the current interface number or the Simple Network Management Protocol (SNMP) MIB-II interface index (ifIndex) value for the interface ID. The advantage to using the SNMP MIB-II ifIndex value is that this number corresponds to the number that the user will see reported by SNMP.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 SNMP ifIndex Value for Interface ID in Data Fields

Before you can use the SNMP ifIndex value for interface identification, OSPF must be configured on the router.

Information About SNMP ifIndex Value for Interface ID in Data Fields

Benefits of Choosing to Identify Interfaces by the SNMP MIB-II ifIndex Value

If you use SNMP for your OSPF network, configuring the OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields feature can be beneficial for the following reasons:

- Using the SNMP MIB-II ifIndex identification numbers to identify OSPF interfaces makes it easier for network administrators to identify interfaces because the numbers will correspond to the numbers that they will see reported by SNMP.
- In the link-state advertisements (LSAs), the value used in fields that have the interface ID will be the same as the value that is reported by SNMP.
- In the output from the **show ipv6 ospf interface** command, the interface ID number will have the same value that is reported by SNMP.
- Using the SNMP MIB-II IfIndex is also suggested, but not required, by the OSPF RFC 2328 for OSPFv2 and the RFC 2740 for OSPFv3.

How OSPFv2 and OSPFv3 Use the SNMP MIB-II ifIndex Value

The user chooses for OSPF interfaces to use the SNMP MIB-II ifIndex number by entering the **interface-id snmp-if-index** command for a specific OSPF process. If an interface under the specific OSPF process does not have an SNMP ifIndex number, OSPF will not be enabled on that interface.

For OSPFv2, the ifIndex number is used for the Link Data field in the Router LSA for unnumbered point-to-point interfaces and sham links. When the **interface-id snmp-if-index** command is entered, the affected LSAs will immediately be reoriginated.

For OSPFv3, the ifIndex number is used for the interface ID in router LSAs, as the LSID in Network and Link LSAs, and also as the interface ID in Hello packets. Intra-Area-Prefix LSAs that reference Network LSAs have the Network LSAs LSID in the Referenced LSID field, so they will also be updated when the **interface-id snmp-if-index** command is entered. The old Network, Link, and Intra-Area-Prefix LSAs that are associated with a Network LSA will be flushed.

For both OSPFv2 and OSPFv3, adjacencies are not flapped, except for affected OSPFv3 demand circuits (including virtual links) with full adjacencies.

For both OSPFv2 and OSPFv3, if an interface does not have an SNMP ifIndex number and an interface ID is needed (for OSPFv2 this applies only to unnumbered interfaces and sham links), an error message will be generated and the interface will be disabled. The interface will be reenabled if the **no interface-id snmp-if-index** command is entered.

How to Configure SNMP ifIndex Value for Interface ID in Data Fields

Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **router ospf** *process-id* [**vrf** *vpn-name*]
   -
   - **ipv6 router ospf** *process-id*
4. **interface-id snmp-if-index**
5. **end**
6. **show snmp mib ifmib ifindex** [*type number*] [**detail**][**free-list**]

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	Do one of the following: • **router ospf** *process-id* [**vrf** *vpn-name*] • • **ipv6 router ospf** *process-id*	Configures an OSPFv2 routing process and enters router configuration mode. Configures an OSPFv3 routing process and enters router configuration mode.

	Command or Action	Purpose

	Example:
	`Router(config)# router ospf 4`
	Example:
	Example:
	`Router(config)# ipv6 router ospf 4`
		Note If you configure an OSPFv3 routing process, that uses IPv6, you must have already enabled IPv6.

Step 4	**interface-id snmp-if-index** **Example:** `Router(config-router)# interface-id snmp-if-index`	Configures OSPF interfaces with the SNMP interface index identification numbers (ifIndex values).
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode. Repeat this task for each OSPF process for which you want the interfaces to use the SNMP MIB-II ifIndex numbers.
Step 6	**show snmp mib ifmib ifindex** [*type number*] [**detail**][**free-list**] **Example:** `Router# show snmp mib ifmib ifindex GigabitEtherent0/0/0`	Displays SNMP interface index identification numbers (ifIndex values) for all the system interfaces or the specified system interface.

Configuration Examples for SNMP ifIndex Value for Interface ID in Data Fields

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2

The following example configures the OSPF interfaces to use the SNMP ifIndex values for the interfaces IDs. The **show snmp mib ifmib ifindex** command confirms that the SNMP MIB-II ifIndex values are used for the interface ID values in the OSPFv2 data fields.

```
Router# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# router ospf 1
Router(config-router)# interface-id snmp-if-index
Router(config-router)# ^Z
Router# show ip ospf 1 1 data router self
OSPF Router with ID (172.16.0.1) (Process ID 1)
Router Link States (Area 1)
LS age: 6
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 172.16.0.1
Advertising Router: 172.16.0.1
LS Seq Number: 80000007
Checksum: 0x63AF
Length: 48
Area Border Router
Number of Links: 2
Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 172.17.0.1
(Link Data) Router Interface address: 0.0.0.53
Number of TOS metrics: 0
TOS 0 Metrics: 64
Link connected to: a Stub Network
(Link ID) Network/subnet number: 192.168.0.11
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metrics: 1
Router# show snmp mib ifmib ifindex serial 13/0

Serial13/0: Ifindex = 53
```

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3

The following example configures the OSPFv3 interfaces to use the SNMP ifIndex values for the interface IDs:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ipv6 router ospf 1
Router(config-router)# interface-id snmp-if-index
```

The output from the **show snmp mib ifmib ifindex** command confirms that the SNMP MIB-II ifIndex values are being used for the interface ID values in the OSPFv2 data fields:

```
Router# show snmp mib ifmib ifindex GigabitEthernet 0/0/0
0/0/0: Ifindex = 5
Router# show ipv6 ospf interface
OSPF_VL0 is up, line protocol is up
  Interface ID 71
  Area 0, Process ID 1, Instance ID 0, Router ID 172.16.0.1
  Network Type VIRTUAL_LINK, Cost: 10
  Configured as demand circuit.
  Run as demand circuit.
  DoNotAge LSA allowed.
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/2/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1  (Hello suppressed)
  Suppress hello for 1 neighbor(s)
GigabitEthernet is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6F02, Interface ID 10
  Area 0, Process ID 1, Instance ID 0, Router ID 172.16.0.1
  Network Type BROADCAST, Cost: 10
```

```
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.0.1, local address FE80::A8BB:CCFF:FE00:6F02
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
GigabitEthernet is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6F01, Interface ID 6
  Area 1, Process ID 1, Instance ID 2, Router ID 172.16.0.1
  Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.16.0.1, local address FE80::A8BB:CCFF:FE00:6F01
  Backup Designated router (ID) 10.0.0.1, local address FE80::A8BB:CCFF:FE00:6E01
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
Router# show ipv6 ospf database network adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Net Link States (Area 1)
  LS age: 144
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Network Links
  Link State ID: 6 (Interface ID of Designated Router)
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x1FC0
  Length: 32
        Attached Router: 172.16.0.1
        Attached Router: 10.0.0.1
Router# show ipv6 ospf database prefix adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Intra Area Prefix Link States (Area 0)
Routing Bit Set on this LSA
LS age: 196
LS Type: Intra-Area-Prefix-LSA
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x6F11
Length: 44
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:2::
  Prefix Length: 64, Options: None, Metric: 10
Intra Area Prefix Link States (Area 1)
  Routing Bit Set on this LSA
  LS age: 161
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0xB6E7
  Length: 52
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:2:0:A8BB:CCFF:FE00:6F02
  Prefix Length: 128, Options: LA , Metric: 0
  Routing Bit Set on this LSA
```

```
  LS age: 151
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 1006
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x6E24
  Length: 44
  Referenced LSA Type: 2002
  Referenced Link State ID: 6
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:1::
  Prefix Length: 64, Options: None, Metric: 0
Router# show ipv6 ospf database router

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
Router Link States (Area 0)
  Routing Bit Set on this LSA
  LS age: 5 (DoNotAge)
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Router Links
  Link State ID: 0
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000004
  Checksum: 0xEE5C
  Length: 40
  Area Border Router
  Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 70
      Neighbor Interface ID: 71
      Neighbor Router ID: 172.16.0.1
LS age: 162
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xCE7C
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Virtual Link
      Link Metric: 10
      Local Interface ID: 71
      Neighbor Interface ID: 70
      Neighbor Router ID: 10.0.0.1
Router Link States (Area 1)
Routing Bit Set on this LSA
LS age: 176
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 10.0.0.1
LS Seq Number: 80000003
Checksum: 0xC807
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
LS age: 175
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xBD10
Length: 40
```

```
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
Router# show ipv6 ospf database link adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Link (Type-8) Link States (Area 0)
  LS age: 245
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Link-LSA (Interface: GigabitEthernet2/0)
  Link State ID: 10 (Interface ID)
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000002
  Checksum: 0xA0CB
  Length: 56
  Router Priority: 1
  Link Local Address: FE80::A8BB:CCFF:FE00:6F02
  Number of Prefixes: 1
  Prefix Address: 2002:0:2::
  Prefix Length: 64, Options: None
Link (Type-8) Link States (Area 1)
LS age: 250
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: GigabitEthernet1/0)
Link State ID: 6 (Interface ID)
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x4F94
Length: 44
Router Priority: 1
Link Local Address: FE80::A8BB:CCFF:FE00:6F01
Number of Prefixes: 0
```

Additional References

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
Protecting TE tunnel interfaces	MPLS Traffic Engineering--Fast Reroute Link and Node Protection section in the *Cisco IOS Multiprotocol Label Switching Configuration Guide*

Standards

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

MIBs

MIB	MIBs Link
• None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 5286	Basic Specification for IP Fast Reroute: Loop-Free Alternates

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

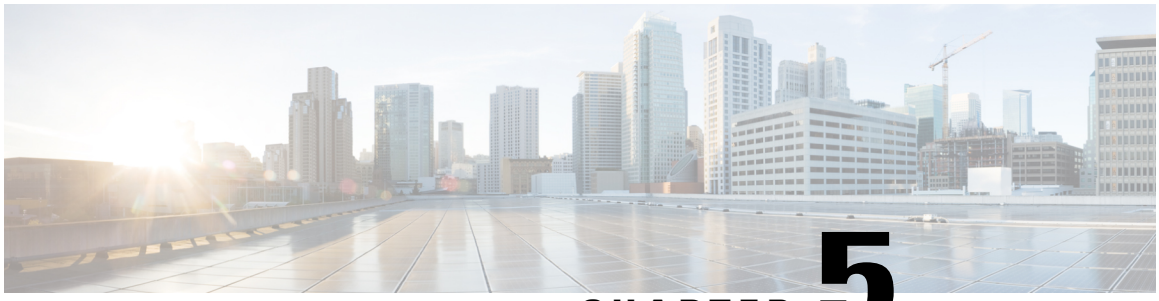
Feature Information for OSPF SNMP ifIndex Value for Interface ID

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 4: Feature Information for OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields

Feature Name	Releases	Feature Information
OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields	Cisco IOS XE Release 2.6 Cisco IOS Release 15.1(1)SG Cisco IOS XE Release 3.3SG	This allows you to choose either the current interface number or the SNMP ifIndex value for the interface ID in OSPFv2 and OSPFv3 data fields. The advantage to using the SNMP MIB-II ifIndex value is that this number corresponds to the number that the user will see reported by SNMP. The following command is introduced or modified by the feature documented in this module: **interface-id snmp-if-index**



CHAPTER 5

OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

This document describes the Open Shortest Path First (OSPF) mechanism to exclude IP prefixes of connected networks from link-state advertisements (LSAs). When OSPF is deployed in large networks, limiting the number of IP prefixes that are carried in the OSPF LSAs can speed up OSPF convergence.

This feature can also be utilized to enhance the security of an OSPF network by allowing the network administrator to prevent IP routing toward internal nodes.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 Excluding Connected IP Prefixes from LSAs

Before you can use the mechanism to exclude IP prefixes from LSAs, the OSPF routing protocol must be configured.

Information About Excluding Connected IP Prefixes from LSAs

One way to improve OSPF network convergence is to limit the number of IP prefixes carried in LSAs.

Previous Methods to Limit the Number of IP Prefixes Carried in LSAs

Configuring interfaces as unnumbered limits IP prefixes. However, for network management and the ease of identifying and troubleshooting numbered interfaces, you might want to have numbered interfaces and also want to limit the number of IP advertisements.

Feature Overview

The OSPF mechanism to exclude connected IP prefixes from LSAs allows network administrators to control what IP prefixes are installed into LSAs. This functionality is implemented for router and network LSAs in the following manner:

- For the router LSA, to exclude prefixes, the feature excludes link type 3 (stub link).
- For the network LSA, the OSPF Designated Router (DR) generates LSAs with a special /32 network mask (0xFFFFFFFF).

Note Previous versions of Cisco IOS software that do not have this feature will install the /32 prefix into the routing table.

Globally Suppressing IP Prefix Advertisements per OSPF Process

You can reduce OSPF convergence time by configuring the OSPF process on a router to prevent the advertisement of all IP prefixes by using the **prefix-suppression** command in router configuration mode.

Note Prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces are excluded because typical network designs require those to remain reachable.

Suppressing IP Prefix Advertisements on a Per-Interface Basis

You can explicitly configure an OSPF interface not to advertise its IP network to its neighbors by using the **ip ospf prefix-suppression** command in interface configuration mode.

Note If you have globally suppressed IP prefixes from connected IP networks by configuring the **prefix-suppression** router configuration command, the interface configuration command takes precedence over the router configuration mode command.

How to Exclude Connected IP Prefixes from OSPF LSAs

This section describes how to configure two alternative methods to suppress IP prefix advertisements. You can suppress IP prefix advertisements per OSPF process or per interface. This section also explains how you can troubleshoot IP prefix suppression.

Excluding IP Prefixes per OSPF Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **prefix-suppression**
5. **end**
6. **show ip ospf**

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	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**prefix-suppression** **Example:** `Router(config-router)# prefix-suppression`	Prevents OSPF from advertising all IP prefixes except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf** **Example:** `Router# show ip ospf`	Displays general information about OSPF routing processes. **Note** Use this command to verify that IP prefix suppression has been enabled.

Examples

In the following example, output from the **show ip ospf** command shows that IP prefix advertisement has been suppressed for OSPF process 1.

```
Router# show ip ospf

Routing Process "ospf 1" with ID 10.0.0.6
Start time: 00:00:04.912, Time elapsed: 00:02:35.184
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
It is an area border router
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 2. Checksum Sum 0x0132C8
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 3 normal 0 stub 0 nssa
Number of areas transit capable is 1
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Prefix-suppression is enabled
.
.
.
```

Excluding IP Prefixes on a Per-Interface Basis

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf prefix-suppression** [**disable**]
5. **end**
6. **show ip ospf interface**

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	**interface** *type number* **Example:** `Router(config)# interface serial 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf prefix-suppression** [**disable**] **Example:** `Router(config-if)# ip ospf prefix-suppression`	Prevents OSPF from advertising IP prefixes that belong to a specific interface, except those that are associated with secondary IP addresses. **Note** When you enter the **ip ospf prefix suppression**command in interface configuration mode, it takes precedence over the **prefix-suppression** command that is entered in router configuration mode.
Step 5	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf interface**	Displays OSPF-related interface information.

	Command or Action	Purpose
	Example: `Router# show ip ospf interface`	**Note** Use this command to verify that IP prefix suppression has been enabled for a specific interface.

Examples

In the following example, the output from the **show ip ospf interface** command verifies that prefix suppression has been enabled for Ethernet interface 0/0.

```
Router# show ip ospf interface

Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.130.2/24, Area 2
  Process ID 1, Router ID 10.0.0.6, Network Type BROADCAST, Cost: 10
  Prefix-suppression is enabled
.
.
.
```

Troubleshooting IP Prefix Suppression

SUMMARY STEPS

1. **enable**
2. **debug ip ospf lsa-generation**
3. **debug condition interface** *interface-type interface-number* [**dlci** *dlci*] [**vc** {*vci* | *vpi* | *vci*}]
4. **show debugging**
5. **show logging** [**slot** *slot-number* | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip ospf lsa-generation** **Example:** `Router# debug ip ospf lsa-generation`	Displays informations about each OSPF LSA generated.

	Command or Action	Purpose
Step 3	**debug condition interface** *interface-type interface-number* [**dlci** *dlci*] [**vc** {*vci* | *vpi* | *vci*}] **Example:** `Router# debug interface serial 0/0`	Limits output for some **debug** commands on the basis of the interface or virtual circuit.
Step 4	**show debugging** **Example:** `Router# show debugging`	Displays information about the types of debugging that are enabled for your router.
Step 5	**show logging** [**slot** *slot-number* | **summary**] **Example:** `Router# show logging`	Displays the state of syslog and the contents of the standard system logging buffer.

Examples

The following sample output from the **debug ip ospf lsa-generation** command verifies that for the Ethernet interface 0/0, IP prefixes from the connected network 192.168.131.0 are excluded.

```
Router# debug ip ospf lsa-generation

OSPF summary lsa generation debugging is on
Router# debug condition interface e0/0
Condition 1 set
Router# show debugging

IP routing:
   OSPF summary lsa generation debugging is on
Condition 1: interface Et0/0 (1 flags triggered)
        Flags: Et0/0
Router# show logging
*Jun  5 21:54:47.295: OSPF: Suppressing 192.168.131.0/24 on Ethernet1/0 from router LSA
*Jun  5 21:54:52.355: OSPF: Suppressing 192.168.131.0/24 on Ethernet1/0 from router LSA
.
.
.
```

Configuration Examples for Excluding Connected IP Prefixes from LSAs

Excluding IP Prefixes from LSAs for an OSPF Process Example

The following example configures IP prefix suppression for OSPF routing process 23.

```
router ospf 23
 prefix-suppression
 end
```

When the **show ip ospf** command is entered, the displayed output verifies that IP prefix suppression has been enabled for OSPF process 23.

```
Router# show ip ospf
outing Process "ospf 23" with ID 10.0.0.6
Start time: 00:00:04.912, Time elapsed: 00:02:35.184
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
It is an area border router
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 2. Checksum Sum 0x0132C8
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 3 normal 0 stub 0 nssa
Number of areas transit capable is 1
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Prefix-suppression is enabled
.
.
.
```

Excluding IP Prefixes from LSAs for a Specified Interface Example

The following example configures the suppression of all IP prefixes that are associated with Ethernet interface 0/0:

```
interface Ethernet 0/0
 ip ospf prefix-suppression
 end
```

When the **show ip ospf interface** command is entered, the displayed output verifies that IP prefix suppression is enabled for Ethernet interface 0/0.

```
Router# show ip ospf interface

Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.130.2/24, Area 2
  Process ID 1, Router ID 10.0.0.6, Network Type BROADCAST, Cost: 10
  Prefix-suppression is enabled
.
.
.
```

Additional References

The following sections provide references related to the OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements feature.

Related Documents

Related Topic	Document Title
OSPF commands: complete command syntax, command mode, command history, command defaults, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
There are no new MIBs that are associated with this feature.	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	--

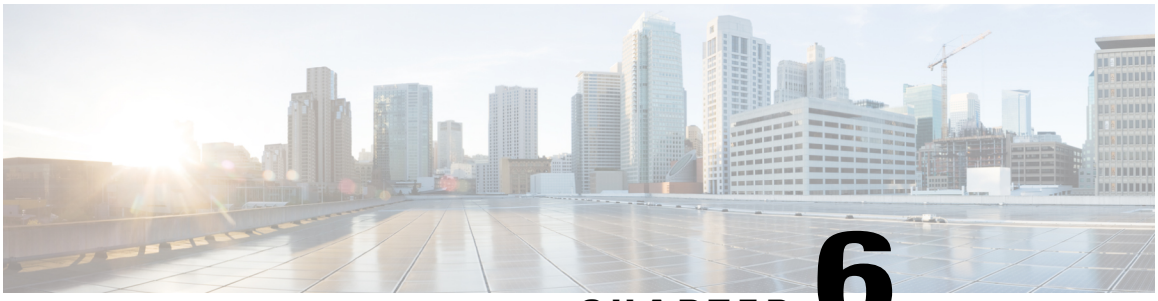
Technical Assistance

Description	Link
The Cisco Support 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

Glossary

network LSA --The link-state advertisement created by the designated router (DR) or pseudonode that represents a group of routers on the same interface. The network LSA advertises summary information to represent the group of routers on the network.

router LSA --The link-state advertisement that is generated by a router. The router LSA advertises routing information (connected routes) for the router.



CHAPTER 6

OSPFv2 Local RIB

With the OSPFv2 Local RIB feature, each OSPF protocol instance has its own local Routing Information Base (RIB). The OSPF local RIB serves as the primary state for OSPF SPF route computation. The global RIB is not updated with intermediate results during the SPF. Instead, the global RIB is updated only when routes are added, deleted, or changed, thereby reducing global RIB computation. This reduced update activity may result in fewer dropped packets.

This feature is enabled by default and does not need to be configured. This document describes some optional configuration tasks to modify how the global and local RIBs function, although it is recommended to keep the default settings.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 OSPFv2 Local RIB

Before this feature is configured, the OSPF routing protocol must be configured.

Restrictions for OSPFv2 Local RIB

This feature is available only for IP Version 4 networks.

Information About OSPFv2 Local RIB

A router that is running OSPFv2 maintains a local RIB in which it stores all routes to destinations that it has learned from its neighbors. At the end of each SPF, OSPF attempts to install the best (that is, the least-cost) routes to a destination present in the local RIB into the global IPv4 routing table. The global RIB will be updated only when routes are added, deleted, or changed. Routes in the local RIB and Forwarding Information Base (FIB) will not compute when intermediate results are computed during SPF, resulting in fewer dropped packets in some circumstances.

By default, the contents of the global RIB are used to compute inter-area summaries, NSSA translation, and forwarding addresses for type-5 and type-7 LSAs. Each of these functions can be configured to use the contents of the OSPF local RIB instead of the global RIB for their computation. Using the local RIB for the computation may be slightly faster in some circumstances, but because the local RIB has information for only a particular instance of OSPF, using it for the computation may yield incorrect results. Potential problems that may occur include routing loops and black-hole routes. It is recommended that you not change the default values because they are conservative and preserve the current global RIB behavior.

By default, OSPF installs discard routes to null0 for any area range (internal) or summary-address (external) prefixes that it advertises to other routers. Installation of a discard route can prevent routing loops in cases where portions of a summary do not have a more specific route in the RIB. Normally, internal discard routes are installed with an administrative distance of 110, while external discard routes have an administrative distance of 254.

There may be rare circumstances, however, when some other values are needed. For example, if one OSPF process installs a route that exactly matches an area range configured on another OSPF process, the internal discard routes for the second OSPF process could be given a higher (less desirable) administrative distance.

How to Configure OSPFv2 Local RIB

Although it is recommended to keep the default settings for the commands described in the following sections, it is optional to change the defaults settings.

Changing the Default Local RIB Criteria

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **local-rib-criteria** [**forwarding-address**] [**inter-area-summary**] [**nssa-translation**]
5. **end**
6. **show ip ospf** *process-id* **rib** [**redistribution**] [*network-prefix*] [*network-mask*] [**detail**]

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	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**local-rib-criteria** [**forwarding-address**] [**inter-area-summary**] [**nssa-translation**] **Example:** `Router(config-router)# local-rib-criteria forwarding-address`	Specifies that the OSPF local RIB will be used for route validation.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**show ip ospf** *process-id* **rib** [**redistribution**] [*network-prefix*] [*network-mask*] [**detail**] **Example:** `Router# show ip ospf 23 rib`	Displays information for the OSPF local RIB or locally redistributed routes.

Changing the Administrative Distance for Discard Routes

Note It is recommended that you keep the default settings. However, you can follow the steps in this section to change the administrative distance for discard routes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **discard-route** [**external** [*distance*]] [**internal** [*distance*]]
5. **end**
6. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]

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.

	Command or Action	Purpose
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**discard-route** [**external** [*distance*]] [**internal** [*distance*]] **Example:** `Router(config-router)# discard-route external 150`	Reinstalls either an external or internal discard route that was previously removed. **Note** You can now specify the administrative distance for internal and external discard routes.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**] **Example:** `Router# show ip route ospf 23`	Displays the current state of the routing table. **Note** Entering the **show ip route** command will verify the changed administrative distance values for external and internal discard routes.

Example

The sample output displayed for the **show ip route** command confirms that the administrative distance for the IP route 192.168.0.0/24 is 110.

```
Router# show ip route 192.168.0.0 255.255.255.0
Routing entry for 192.168.0.0/24
    Known via "ospf 1", distance 110, metric 0, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 0, traffic share count is 1
```

Troubleshooting Tips

You can research the output from the **debug ip ospf rib** command to learn about the function of the local RIB and the interaction between the route redistribution process and the global RIB. For example, you can learn why the routes that OSPF placed in the global RIB are not the same ones that you anticipated.

Configuration Examples for OSPFv2 Local RIB

Example: Changing the Default Local RIB Criteria

In the following example, the **local-rib-criteria** command is entered without any keywords to specify that the local RIB will be used as criteria for all of the following options: forwarding address, inter-area summary, and NSSA translation.

```
router ospf 1
 router-id 10.0.0.6
 local-rib-criteria
```

Example: Changing the Administrative Distance for Discard Routes

In the following example, the administrative distance for external and internal discard routes is set to 25 and 30, respectively.

```
router ospf 1
 router-id 10.0.0.6
 log-adjacency-changes
 discard-route external 25 internal 30
 area 4 range 10.2.0.0 255.255.0.0
 summary-address 192.168.130.2 255.255.255.0
 redistribute static subnets
 network 192.168.129.2 0.255.255.255 area 0
 network 192.168.130.12 0.255.255.255 area 0
```

The output from the **show ip route** command verifies that the administrative distance for the internal route 10.2.0.0/16 is set to 30.

```
Router# show ip route 10.2.0.0 255.255.0.0
Routing entry for 10.2.0.0/16
Known via "ospf 1", distance 30, metric 1, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 1, traffic share count is 1
```

The output from the **show ip route** command verifies that the administrative distance for the external route 192.168.130.2/24 is set to 25.

```
Router# show ip route 192.168.130.2 255.255.255.0
Routing entry for 192.168.130.2/24
 Known via "ospf 1", distance 25, metric 20, type intra area
  Routing Descriptor Blocks:
  * directly connected, via Null0
      Route metric is 20, traffic share count is 1
```

Additional References

The following sections provide references related to OSPFv2 Local RIB.

Related Documents

Related Topic	Document Title
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
None	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE 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 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

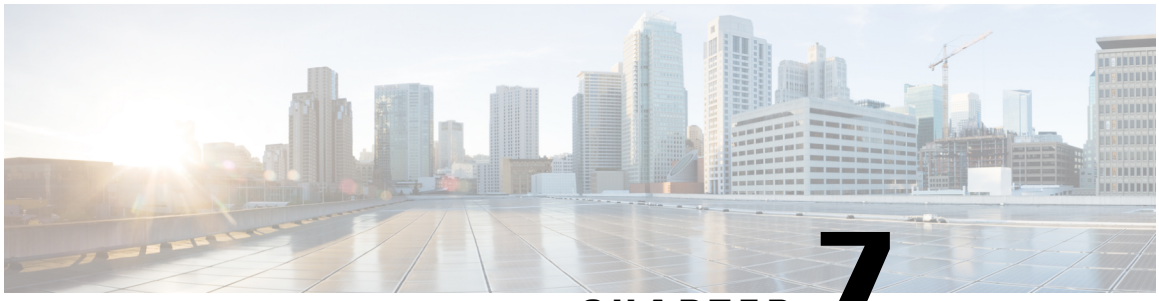
Feature Information for OSPFv2 Local RIB

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 5: Feature Information for the OSPFv2 Local RIB

Feature Name	Releases	Feature Information
OSPFv2 Local RIB	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.3SG	With the OSPFv2 Local RIB feature, each OSPF protocol instance has its own local Routing Information Base (RIB). The OSPF local RIB serves as the primary state for OSPF SPF route computation. The global RIB is not updated with intermediate results during the SPF. Instead, the global RIB is updated only when routes are added, deleted, or changed, thereby reducing global RIB computation. This reduced update activity may result in fewer dropped packets. This feature is enabled by default and does not need to be configured. This document describes some optional configuration tasks to modify how the global and local RIBs function, although it is recommended to keep the default settings. The following commands were introduced or modified: **debug ip ospf rib**, **discard-route**, **local-rib-criteria**, **show ip ospf rib**.



CHAPTER 7

IPv6 Routing: OSPFv3

Open Shortest Path First version 3 (OSPFv3) is an IPv4 and IPv6 link-state routing protocol that supports IPv6 and IPv4 unicast address families (AFs).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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 IPv6 Routing: OSPFv3

- Complete the OSPFv3 network strategy and planning for your IPv6 network. For example, you must decide whether multiple areas are required.
- Enable IPv6 unicast routing.
- Enable IPv6 on the interface.

Restrictions for IPv6 Routing: OSPFv3

When running a dual-stack IP network with OSPF version 2 for IPv4 and OSPFv3, be careful when changing the defaults for commands used to enable OSPFv3. Changing these defaults may affect your OSPFv3 network, possibly adversely.

Information About IPv6 Routing: OSPFv3

How OSPFv3 Works

OSPFv3 is a routing protocol for IPv4 and IPv6. It is a link-state protocol, as opposed to a distance-vector protocol. Think of a link as being an interface on a networking device. A link-state protocol makes its routing decisions based on the states of the links that connect source and destination machines. The state of a link is a description of that interface and its relationship to its neighboring networking devices. The interface information includes the IPv6 prefix of the interface, the network mask, the type of network it is connected to, the devices connected to that network, and so on. This information is propagated in various type of link-state advertisements (LSAs).

A device's collection of LSA data is stored in a link-state database. The contents of the database, when subjected to the Dijkstra algorithm, result in the creation of the OSPF routing table. The difference between the database and the routing table is that the database contains a complete collection of raw data; the routing table contains a list of shortest paths to known destinations via specific device interface ports.

OSPFv3, which is described in RFC 5340, supports IPv6 and IPv4 unicast AFs.

Comparison of OSPFv3 and OSPF Version 2

Much of OSPF version 3 is the same as in OSPF version 2. OSPFv3, which is described in RFC 5340, expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses.

In OSPFv3, a routing process does not need to be explicitly created. Enabling OSPFv3 on an interface will cause a routing process, and its associated configuration, to be created.

In OSPFv3, each interface must be enabled using commands in interface configuration mode. This feature is different from OSPF version 2, in which interfaces are indirectly enabled using the device configuration mode.

When using a nonbroadcast multiaccess (NBMA) interface in OSPFv3, you must manually configure the device with the list of neighbors. Neighboring devices are identified by their device ID.

In IPv6, you can configure many address prefixes on an interface. In OSPFv3, all address prefixes on an interface are included by default. You cannot select some address prefixes to be imported into OSPFv3; either all address prefixes on an interface are imported, or no address prefixes on an interface are imported.

Unlike OSPF version 2, multiple instances of OSPFv3 can be run on a link.

OSPF automatically prefers a loopback interface over any other kind, and it chooses the highest IP address among all loopback interfaces. If no loopback interfaces are present, the highest IP address in the device is chosen. You cannot tell OSPF to use any particular interface.

LSA Types for OSPFv3

The following list describes LSA types, each of which has a different purpose:

- Device LSAs (Type 1)—Describes the link state and costs of a device's links to the area. These LSAs are flooded within an area only. The LSA indicates if the device is an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR), and if it is one end of a virtual link. Type 1 LSAs are also used to advertise stub networks. In OSPFv3, these LSAs have no address information and are network-protocol-independent. In OSPFv3, device interface information may be spread across multiple device LSAs. Receivers must concatenate all device LSAs originated by a given device when running the SPF calculation.
- Network LSAs (Type 2)—Describes the link-state and cost information for all devices attached to the network. This LSA is an aggregation of all the link-state and cost information in the network. Only a designated device tracks this information and can generate a network LSA. In OSPFv3, network LSAs have no address information and are network-protocol-independent.
- Interarea-prefix LSAs for ABRs (Type 3)—Advertises internal networks to devices in other areas (interarea routes). Type 3 LSAs may represent a single network or a set of networks summarized into one advertisement. Only ABRs generate summary LSAs. In OSPFv3, addresses for these LSAs are expressed as *prefix*, *prefix length* instead of *address*, *mask*. The default route is expressed as a prefix with length 0.
- Interarea-device LSAs for ASBRs (Type 4)—Advertises the location of an ASBR. Devices that are trying to reach an external network use these advertisements to determine the best path to the next hop. Type 4 LSAs are generated by ABRs on behalf of ASBRs.
- Autonomous system external LSAs (Type 5)—Redistributes routes from another autonomous system, usually from a different routing protocol into OSPFv3. In OSPFv3, addresses for these LSAs are expressed as *prefix*, *prefix length* instead of *address*, *mask*. The default route is expressed as a prefix with length 0.
- Link LSAs (Type 8)—Have local-link flooding scope and are never flooded beyond the link with which they are associated. Link LSAs provide the link-local address of the device to all other devices attached to the link, inform other devices attached to the link of a list of prefixes to associate with the link, and allow the device to assert a collection of Options bits to associate with the network LSA that will be originated for the link.
- Intra-Area-Prefix LSAs (Type 9)—A device can originate multiple intra-area-prefix LSAs for each device or transit network, each with a unique link-state ID. The link-state ID for each intra-area-prefix LSA describes its association to either the device LSA or the network LSA and contains prefixes for stub and transit networks.

An address prefix occurs in almost all newly defined LSAs. The prefix is represented by three fields: PrefixLength, PrefixOptions, and Address Prefix. In OSPFv3, addresses for these LSAs are expressed as *prefix*, *prefix length* instead of *address*, *mask*. The default route is expressed as a prefix with length 0. Type 3 and Type 9 LSAs carry all prefix (subnet) information that, in OSPFv2, is included in device LSAs and network LSAs. The Options field in certain LSAs (device LSAs, network LSAs, interarea-device LSAs, and link LSAs) has been expanded to 24 bits to provide support for OSPFv3.

In OSPFv3, the sole function of the link-state ID in interarea-prefix LSAs, interarea-device LSAs, and autonomous-system external LSAs is to identify individual pieces of the link-state database. All addresses or device IDs that are expressed by the link-state ID in OSPF version 2 are carried in the body of the LSA in OSPFv3.

The link-state ID in network LSAs and link LSAs is always the interface ID of the originating device on the link being described. For this reason, network LSAs and link LSAs are now the only LSAs whose size cannot be limited. A network LSA must list all devices connected to the link, and a link LSA must list all of the address prefixes of a device on the link.

NBMA in OSPFv3

On NBMA networks, the designated router (DR) or backup DR (BDR) performs the LSA flooding. On point-to-point networks, flooding simply goes out an interface directly to a neighbor.

Devices that share a common segment (Layer 2 link between two interfaces) become neighbors on that segment. OSPFv3 uses the Hello protocol, periodically sending hello packets out each interface. Devices become neighbors when they see themselves listed in the neighbor's hello packet. After two devices become neighbors, they may proceed to exchange and synchronize their databases, which creates an adjacency. Not all neighboring devices have an adjacency.

On point-to-point and point-to-multipoint networks, the software floods routing updates to immediate neighbors. There is no DR or BDR; all routing information is flooded to each networking device.

On broadcast or NBMA segments only, OSPFv3 minimizes the amount of information being exchanged on a segment by choosing one device to be a DR and one device to be a BDR. Thus, the devices on the segment have a central point of contact for information exchange. Instead of each device exchanging routing updates with every other device on the segment, each device exchanges information with the DR and BDR. The DR and BDR relay the information to the other devices.

The software looks at the priority of the devices on the segment to determine which devices will be the DR and BDR. The device with the highest priority is elected the DR. If there is a tie, then the device with the higher device ID takes precedence. After the DR is elected, the BDR is elected the same way. A device with a device priority set to zero is ineligible to become the DR or BDR.

When using NBMA in OSPFv3, you cannot automatically detect neighbors. On an NBMA interface, you must configure your neighbors manually using interface configuration mode.

Load Balancing in OSPFv3

When a device learns multiple routes to a specific network via multiple routing processes (or routing protocols), it installs the route with the lowest administrative distance in the routing table. Sometimes the device must select a route from among many learned via the same routing process with the same administrative distance. In this case, the device chooses the path with the lowest cost (or metric) to the destination. Each routing process calculates its cost differently and the costs may need to be manipulated in order to achieve load balancing.

OSPFv3 performs load balancing automatically in the following way. If OSPFv3 finds that it can reach a destination through more than one interface and each path has the same cost, it installs each path in the routing table. The only restriction on the number of paths to the same destination is controlled by the **maximum-paths** command. The default maximum paths is 16, and the range is from 1 to 64.

Addresses Imported into OSPFv3

When importing the set of addresses specified on an interface on which OSPFv3 is running into OSPFv3, you cannot select specific addresses to be imported. Either all addresses are imported, or no addresses are imported.

OSPFv3 Customization

You can customize OSPFv3 for your network, but you likely will not need to do so. The defaults for OSPFv3 are set to meet the requirements of most customers and features. If you must change the defaults, refer to the IPv6 command reference to find the appropriate syntax.

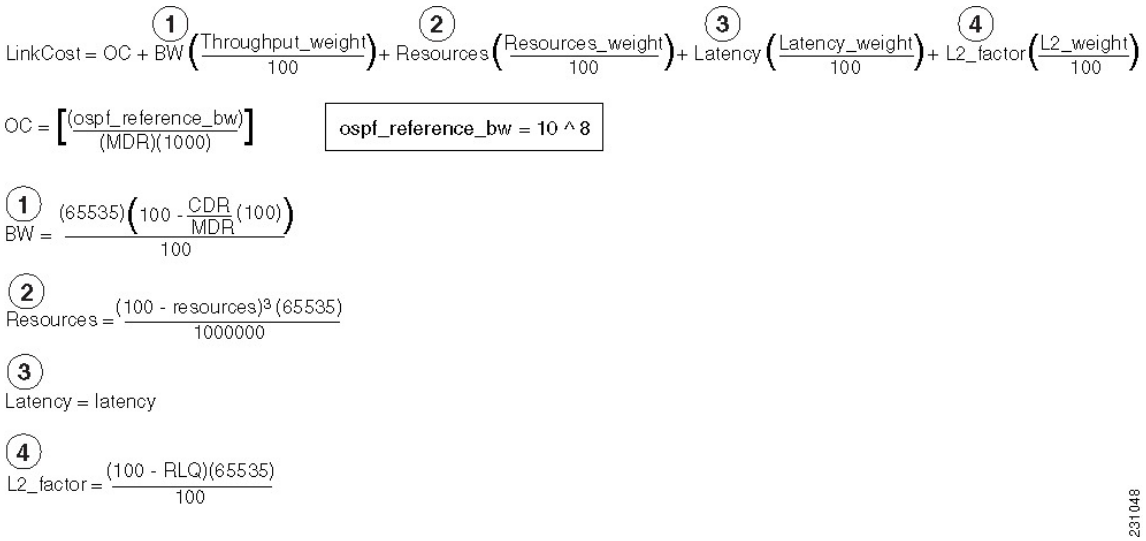
Caution Be careful when changing the defaults. Changing defaults will affect your OSPFv3 network, possibly adversely.

OSPFv3 Cost Calculation

Because cost components can change rapidly, it might be necessary to reduce the volume of changes to reduce network-wide churn. The recommended values for S2, S3, and S4 in the second table below are based on network simulations that may reduce the rate of network changes. The recommended value for S1 is 0 to eliminate this variable from the route cost calculation.

The overall link cost is computed using the formula shown in the figure below.

Figure 1: Overall Link Cost Formula



The table below defines the symbols used in the OSPFv3 cost calculation.

Table 6: OSPFv3 Cost Calculation Definitions

Cost Component	Component Definition
OC	The default OSPFv3 cost. Calculated from reference bandwidth using reference_bw / (MDR*1000), where reference_bw=10^8.

Cost Component	Component Definition
A through D	Various radio-specific data-based formulas that produce results in the 0 through 64,000 range.
A	CDR- and MDR-related formula: (2^16 * (100 – (CDR * 100 / MDR)))/100
B	Resources related formula: ((100 – RESOURCES)^3 * 2^16 / 10^6)
C	Latency as reported by the radio, already in the 0 through 64,000 range when reported (LATENCY).
D	RLF-related formula: ((100 – RLF) * 2^16)/100
S1 through S4	Scalar weighting factors input from the CLI. These scalars scale down the values as computed by A through D. The value of 0 disables and the value of 100 enables full 0 through 64,000 range for one component.

Because each network might have unique characteristics that require different settings to optimize actual network performance, these are recommended values intended as a starting point for optimizing an OSPFv3 network. The table below lists the recommended value settings for OSPFv3 cost metrics.

Table 7: Recommended Value Settings for OSPFv3 Cost Metrics

Setting	Metric Description	Default Value	Recommended Value
S1	ipv6 ospf dynamic weight throughout	100	0
S2	ipv6 ospf dynamic weight resources	100	29
S3	ipv6 ospf dynamic weight latency	100	29
S4	ipv6 ospf dynamic weight L2 factor	100	29

The default path costs were calculated using this formula, as noted in the following list. If these values do not suit your network, you can use your own method of calculating path costs.

- 56-kbps serial link—Default cost is 1785.

- 64-kbps serial link—Default cost is 1562.
- T1 (1.544-Mbps serial link)—Default cost is 64.
- E1 (2.048-Mbps serial link)—Default cost is 48.
- 4-Mbps Token Ring—Default cost is 25.
- Ethernet—Default cost is 10.
- 16-Mbps Token Ring—Default cost is 6.
- FDDI—Default cost is 1.
- X25—Default cost is 5208.
- Asynchronous—Default cost is 10,000.
- ATM—Default cost is 1.

To illustrate these settings, the following example shows how OSPFv3 cost metrics might be defined for a Virtual Multipoint Interface (VMI) interface:

```
interface vmi1
 ipv6 ospf cost dynamic weight throughput 0
 ipv6 ospf cost dynamic weight resources 29
 ipv6 ospf cost dynamic weight latency 29
 ipv6 ospf cost dynamic weight L2-factor 29
```

Force SPF in OSPFv3

When the **process** keyword is used with the **clear ipv6 ospf** command, the OSPFv3 database is cleared and repopulated, and then the SPF algorithm is performed. When the **force-spf** keyword is used with the **clear ipv6 ospf** command, the OSPFv3 database is not cleared before the SPF algorithm is performed.

How to Configure Load Balancing in OSPFv3

Configuring the OSPFv3 Device Process

Once you have completed step 3 and entered OSPFv3 router configuration mode, you can perform any of the subsequent steps in this task as needed to configure OSPFv3 Device configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **area** *area-ID* [**default-cost** | **nssa** | **stub**]
5. **auto-cost reference-bandwidth** *Mbps*
6. **bfd all-interfaces**
7. **default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]
8. **ignore lsa mospf**
9. **interface-id snmp-if-index**
10. **log-adjacency-changes** [**detail**]
11. **passive-interface** [**default** | *interface-type interface-number*]
12. **queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**}
13. **router-id** *router-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 1`	Enters router configuration mode for the IPv4 or IPv6 address family.
Step 4	**area** *area-ID* [**default-cost**	**nssa**	**stub**] **Example:** `Device(config-router)# area 1`	Configures the OSPFv3 area.

	Command or Action	Purpose
Step 5	**auto-cost reference-bandwidth** *Mbps* **Example:** `Device(config-router)# auto-cost reference-bandwidth 1000`	Controls the reference value OSPFv3 uses when calculating metrics for interfaces in an IPv4 OSPFv3 process.
Step 6	**bfd all-interfaces** **Example:** `Device(config-router)# bfd all-interfaces`	Enables BFD for an OSPFv3 routing process
Step 7	**default** {**area** *area-ID* [**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*] **Example:** `Device(config-router)# default area 1`	Returns an OSPFv3 parameter to its default value.
Step 8	**ignore lsa mospf** **Example:** `Device(config-router)# ignore lsa mospf`	Suppresses the sending of syslog messages when the device receives LSA Type 6 multicast OSPFv3 packets, which are unsupported.
Step 9	**interface-id snmp-if-index** **Example:** `Device(config-router)# interface-id snmp-if-index`	Configures OSPFv3 interfaces with Simple Network Management Protocol (SNMP) MIB-II interface Index (ifIndex) identification numbers in IPv4 and IPv6.
Step 10	**log-adjacency-changes** [**detail**] **Example:** `Device(config-router)# log-adjacency-changes`	Configures the device to send a syslog message when an OSPFv3 neighbor goes up or down.
Step 11	**passive-interface** [**default** | *interface-type interface-number*] **Example:** `Device(config-router)# passive-interface default`	Suppresses sending routing updates on an interface when an IPv4 OSPFv3 process is used.

	Command or Action	Purpose
Step 12	**queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**} **Example:** `Device(config-router)# queue-depth update 1500`	Configures the number of incoming packets that the IPv4 OSPFv3 process can keep in its queue.
Step 13	**router-id** *router-id* **Example:** `Device(config-router)# router-id 10.1.1.1`	Enter this command to use a fixed router ID.

Configuring NBMA Interfaces in OSPFv3

You can customize OSPFv3 in your network to use NBMA interfaces. OSPFv3 cannot automatically detect neighbors over NBMA interfaces. On an NBMA interface, you must configure your neighbors manually using interface configuration mode.

Before You Begin

Before you configure NBMA interfaces, you must perform the following tasks:

- Configure your network to be an NBMA network
- Identify each neighbor

Note

- You cannot automatically detect neighbors when using NBMA interfaces. You must manually configure your device to detect neighbors when using an NBMA interface.
- When the **ipv6 ospf neighbor** command is configured, the IPv6 address used must be the link-local address of the neighbor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}]
5. **ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface serial 0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	**frame-relay map ipv6** *ipv6-address dlci* [**broadcast**] [**cisco**] [**ietf**] [**payload-compression** {**packet-by-packet** | **frf9 stac** [*hardware-options*] | **data-stream stac** [*hardware-options*]}] **Example:** `Device(config-if)# frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120`	Defines the mapping between a destination IPv6 address and the data-link connection identifier (DLCI) used to connect to the destination address. • In this example, the NBMA link is Frame Relay. For other kinds of NBMA links, different mapping commands are used.
Step 5	**ipv6 ospf neighbor** *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**] **Example:** `Device(config-if) ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01`	Configures an OSPFv3 neighboring device.

Forcing an SPF Calculation

SUMMARY STEPS

1. **enable**
2. **clear ospfv3** [*process-id*] **force-spf**
3. **clear ospfv3** [*process-id*] **process**
4. **clear ospfv3** [*process-id*] **redistribution**
5. **clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear ospfv3** [*process-id*] **force-spf** **Example:** `Device# clear ospfv3 1 force-spf`	Runs SPF calculations for an OSPFv3 process. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 3	**clear ospfv3** [*process-id*] **process** **Example:** `Device# clear ospfv3 2 process`	Resets an OSPFv3 process. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 4	**clear ospfv3** [*process-id*] **redistribution** **Example:** `Device# clear ospfv3 redistribution`	Clears OSPFv3 route redistribution. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration. • Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.
Step 5	**clear ipv6 ospf** [*process-id*] {**process** | **force-spf** | **redistribution**} **Example:** `Device# clear ipv6 ospf force-spf`	Clears the OSPFv3 state based on the OSPFv3 routing process ID, and forces the start of the SPF algorithm. • If the **clear ospfv3 force-spf** command is configured, it overwrites the **clear ipv6 ospf** configuration.

	Command or Action	Purpose
		• Once the **clear ospfv3 force-spf** command has been used, the **clear ipv6 ospf** command cannot be used.

Verifying OSPFv3 Configuration and Operation

This task is optional, and the commands can be entered in any order, as needed.

SUMMARY STEPS

1. **enable**
2. **show ospfv3** [*process-id*] [*address-family*] **border-routers**
3. **show ospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**]
4. **show ospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**]
5. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number*
6. **show ospfv3** [*process-id*] [*address-family*] **graceful-restart**
7. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**]
8. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]
9. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list**[*neighbor*] [*interface*] [*interface-neighbor*]
10. **show ospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]
11. **show ospfv3** [*process-id*] [*address-family*] **statistic** [**detail**]
12. **show ospfv3** [*process-id*] [*address-family*] **summary-prefix**
13. **show ospfv3** [*process-id*] [*address-family*] **timers rate-limit**
14. **show ospfv3** [*process-id*] [*address-family*] **traffic**[*interface-type interface-number*]
15. **show ospfv3** [*process-id*] [*address-family*] **virtual-links**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**show ospfv3** [*process-id*] [*address-family*] **border-routers** **Example:** `Device# show ospfv3 border-routers`	Displays the internal OSPFv3 routing table entries to an ABR and ASBR.
Step 3	**show ospfv3** [*process-id* [*area-id*]] [*address-family*] **database** [**database-summary** | **internal** | **external** [*ipv6-prefix*] [*link-state-id*] | **grace** | **inter-area prefix** [*ipv6-prefix* | *link-state-id*] | **inter-area router** [*destination-router-id* | *link-state-id*] | **link** [**interface** *interface-name* | *link-state-id*] | **network** [*link-state-id*] | **nssa-external** [*ipv6-prefix*] [*link-state-id*] | **prefix** [**ref-lsa** {**router** | **network**} | *link-state-id*] | **promiscuous** | **router** [*link-state-id*] | **unknown** [{**area** | **as** | **link**} [*link-state-id*]] [**adv-router** *router-id*] [**self-originate**] **Example:** `Device# show ospfv3 database`	Displays lists of information related to the OSPFv3 database for a specific device.
Step 4	**show ospfv3** [*process-id*] [*address-family*] **events** [**generic** | **interface** | **lsa** | **neighbor** | **reverse** | **rib** | **spf**] **Example:** `Device# show ospfv3 events`	Displays detailed information about OSPFv3 events.
Step 5	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **flood-list** *interface-type interface-number* **Example:** `Device# show ospfv3 flood-list`	Displays a list of OSPFv3 LSAs waiting to be flooded over an interface.
Step 6	**show ospfv3** [*process-id*] [*address-family*] **graceful-restart** **Example:** `Device# show ospfv3 graceful-restart`	Displays OSPFv3 graceful restart information.
Step 7	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **interface** [*type number*] [**brief**] **Example:** `Device# show ospfv3 interface`	Displays OSPFv3-related interface information.

	Command or Action	Purpose
Step 8	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**] **Example:** `Device# show ospfv3 neighbor`	Displays OSPFv3 neighbor information on a per-interface basis.
Step 9	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **request-list**[*neighbor*] [*interface*] [*interface-neighbor*] **Example:** `Device# show ospfv3 request-list`	Displays a list of all LSAs requested by a device.
Step 10	**show ospfv3** [*process-id*] [*area-id*] [*address-family*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*] **Example:** `Device# show ospfv3 retransmission-list`	Displays a list of all LSAs waiting to be re-sent.
Step 11	**show ospfv3** [*process-id*] [*address-family*] **statistic** [**detail**] **Example:** `Device# show ospfv3 statistics`	Displays OSPFv3 SPF calculation statistics.
Step 12	**show ospfv3** [*process-id*] [*address-family*] **summary-prefix** **Example:** `Device# show ospfv3 summary-prefix`	Displays a list of all summary address redistribution information configured under an OSPFv3 process.
Step 13	**show ospfv3** [*process-id*] [*address-family*] **timers rate-limit** **Example:** `Device# show ospfv3 timers rate-limit`	Displays all of the LSAs in the rate limit queue.
Step 14	**show ospfv3** [*process-id*] [*address-family*] **traffic**[*interface-type interface-number*] **Example:** `Device# show ospfv3 traffic`	Displays OSPFv3 traffic statistics.
Step 15	**show ospfv3** [*process-id*] [*address-family*] **virtual-links** **Example:** `Device# show ospfv3 virtual-links`	Displays parameters and the current state of OSPFv3 virtual links.

Configuration Examples for Load Balancing in OSPFv3

Example: Configuring the OSPFv3 Device Process

```
Device# show ospfv3 database
            OSPFv3 Device with ID (172.16.4.4) (Process ID 1)
                Device Link States (Area 0)
ADV Device         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Device Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Dest DevID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
            Intra Area Prefix Link States (Area 0)
ADV Device         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0


Device# show ospfv3 neighbor

OSPFv3 Device with ID (10.1.1.1) (Process ID 42)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.4.4.4        1    FULL/  -        00:00:39    12              vm1
OSPFv3 Device with ID (10.2.1.1) (Process ID 100)
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
10.5.4.4          1    FULL/  -        00:00:35    12              vm1
```

Example: Configuring NBMA Interfaces

The following example shows how to configure an OSPFv3 neighboring device with the IPv6 address of FE80::A8BB:CCFF:FE00:C01.

```
interface serial 0
 ipv6 enable
 ipv6 ospf 1 area 0
 encapsulation frame-relay
 frame-relay map ipv6 FE80::A8BB:CCFF:FE00:C01 120
 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C0
```

Example: Forcing SPF Configuration

The following example shows how to trigger SPF to redo the SPF and repopulate the routing tables:

```
clear ipv6 ospf force-spf
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
IPv6 Routing: OSPFv3	"*Configuring OSPF*" module

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

MIBs

MIB	MIBs Link
	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

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

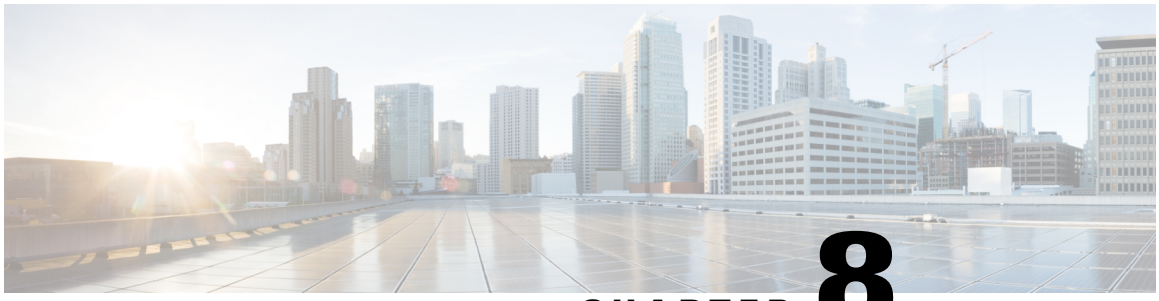
Feature Information for IPv6 Routing: OSPFv3

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 8: Feature Information for IPv6 Routing: OSPFv3

Feature Name	Releases	Feature Information
IPv6 Routing: OSPFv3	12.2(15)T 12.3 12.2(25)SEA 12.2(25)SG 3.2.0SG 15.0(2)SG 12.2(33)SRA 12.2(17a)SX1 Cisco IOS XE Release 2.1	OSPF version 3 for IPv6 expands on OSPF version 2 to provide support for IPv6 routing prefixes and the larger size of IPv6 addresses.
OSPFv3 Dynamic Interface Cost Support	12.4(15)T	OSPFv3 dynamic interface cost support provides enhancements to the OSPFv3 cost metric for supporting mobile ad hoc networking.



CHAPTER 8

TTL Security Support for OSPFv3 on IPv6

The Time To Live (TTL) Security Support for Open Shortest Path First version 3 (OSPFv3) on IPv6 feature increases protection against OSPFv3 denial of service attacks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 module.

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.

Restrictions for TTL Security Support for OSPFv3 on IPv6

- OSPFv3 TTL security can be configured for virtual and sham links only.
- OSPFv3 TTL security must be configured in IPv6 address family configuration mode (config-router-af). To enter IPv6 address family configuration mode you use the **address-family ipv6** command.
- Sham links must not be configured on the default Virtual Routing and Forwarding (VRF).

Prerequisites for TTL Security Support for OSPFv3 on IPv6

The TTL Security Support for OSPFv3 on IPv6 feature is available only on platforms with OSPFv3 routing capabilities.

Information About TTL Security Support for OSPFv3 on IPv6

OSPFv3 TTL Security Support for Virtual and Sham Links

In OSPFv3, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a virtual link. The virtual link must be configured in the two devices you want to use to connect the partitioned backbone. The configuration information in each device consists of the other virtual endpoint (the other Area Border Router [ABR]) and the nonbackbone area that the two devices have in common (called the transit area.) Note that virtual links cannot be configured through stub areas. Sham links are similar to virtual links in many ways, but sham links are used in Layer 3 Multiprotocol Label Switching (MPLS) VPN networks to connect provider edge (PE) routers across the MPLS backbone.

Note Multihop adjacencies such as virtual links and sham links use global IPv6 addresses that require you to configure TTL security to control the number of hops that a packet can travel.

If TTL security is enabled, OSPFv3 sends outgoing packets with an IP header TTL value of 255 and discards incoming packets that have TTL values less than the configurable threshold. Because each device that forwards an IP packet decreases the TTL value, packets received via a direct (one-hop) connection will have a value of 255. Packets that cross two hops will have a value of 254, and so on. The receive threshold is configured in terms of the maximum number of hops that a packet may have traveled. The value for this *hop-count* argument is a number from 1 to 254, with a default of 1.

To establish a virtual link or a sham link, use the **area virtual-link** or **area sham-link cost** commands respectively. To configure TTL security on a virtual link or a sham link, configure the **ttl-security** keyword and the *hop-count* argument in either command. Note that the *hop-count* argument value is mandatory in this case.

Note OSPFv3 TTL Security can be configured for virtual and sham links only, and must be configured in address family configuration (config-router-af) mode for IPv6 address families.

How to Configure TTL Security Support for OSPFv3 on IPv6

Configuring TTL Security Support on Virtual Links for OSPFv3 on IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast vrf** *vrf-name*
5. **area** *area-ID* **virtual-link** *router-id* **ttl-security hops** *hop-count*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 1`	Enables router configuration mode for the IPv4 or IPv6 address family.
Step 4	**address-family ipv6 unicast vrf** *vrf-name* **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Enters address family configuration mode for OSPFv3, specifies IPv6 unicast address prefixes, and specifies the name of the VRF instance to associate with subsequent address family configuration mode commands.

	Command or Action	Purpose
Step 5	**area** *area-ID* **virtual-link** *router-id* **ttl-security hops** *hop-count* **Example:** `Device(config-router-af)# area 1 virtual-link 10.1.1.1 ttl-security hops 10`	Defines an OSPFv3 virtual link and configures TTL security on the virtual link.
Step 6	**end** **Example:** `Device(config-router-af)# end`	(Optional) Returns to privileged EXEC mode.

Configuring TTL Security Support on Sham Links for OSPFv3 on IPv6

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast vrf** *vrf-name*
5. **area** *area-id* **sham-link** *source-address destination-address* **ttl-security hops** *hop-count*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**address-family ipv6 unicast vrf** *vrf-name* **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Enters address family configuration mode for OSPFv3, specifies IPv6 unicast address prefixes, and specifies the name of the VRF instance to associate with subsequent address family configuration mode commands.
Step 5	**area** *area-id* **sham-link** *source-address destination-address* **ttl-security hops** *hop-count* **Example:** `Device(config-router-af)# area 1 sham-link 2001:DB8:1::1 2001:DB8:0:A222::2 ttl-security hops 10`	Defines an OSPFv3 sham link and configures TTL security on the sham link.
Step 6	**end** **Example:** `Device(config-router-af)# end`	(Optional) Returns to privileged EXEC mode.

Configuration Examples for TTL Security Support for OSPFv3 on IPv6

Example: TTL Security Support on Virtual Links for OSPFv3 on IPv6

The following example shows how to configure TTL virtual link security:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast vrf vrf1
Device(config-router-af)# area 1 virtual-link 10.1.1.1 ttl-security hops 10
Device(config-router-af)# end
Device# show ospfv3 virtual-links
OSPFv3 1 address-family ipv6 (router-id 10.1.1.7)
Virtual Link OSPFv3_VL0 to router 10.1.1.2 is down
  Interface ID 23, IPv6 address ::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, Cost of using 65535
  Transmit Delay is 1 sec, State DOWN,
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Strict TTL checking enabled, up to 10 hops allowed
```

Example: TTL Security Support on Sham Links for OSPFv3 on IPv6

The following example shows how to configure TTL sham link security:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast vrf vrf1
Device(config-router-af)# area 1 sham-link 2001:DB8:1::1 2001:DB8:0:A222::2 ttl-security
hops 10
Device(config-router-af)# end
Device#
```

Additional References

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
IPv6 routing: OSPFv3	"IPv6 Routing: OSPFv3" module

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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 TTL Security Support for OSPFv3 on IPv6

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 9: TTL Security Support for OSPFv3 on IPv6

Feature Name	Software Releases	Feature Information
TTL Security Support for OSPFv3 on IPv6	Cisco IOS Release 15.2(4)S Cisco IOS XE Release 3.7S Cisco IOS Release 15.1(1)SY Cisco IOS Release 15.3(1)T Cisco IOS XE Release 3.4SG	The TTL Security Support for OSPFv3 on IPv6 feature increases protection against OSPFv3 denial of service attacks. The following commands were introduced or modified by this feature: **area sham-link**, **area virtual-link**.