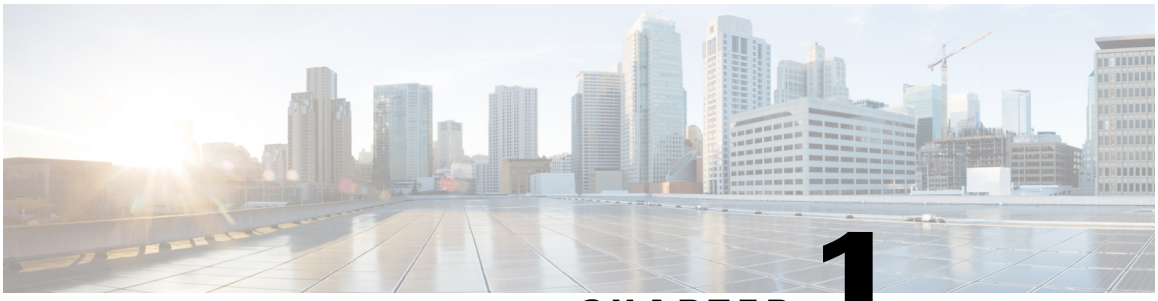
IP Routing: OSPF Configuration Guide

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



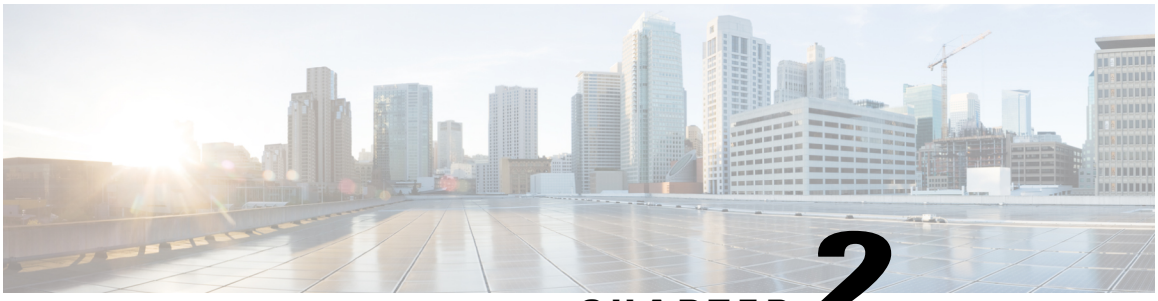
CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E (for Catalyst Switching) and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Note The Feature Information table in the technology configuration guide mentions when a feature was introduced. It might or might not mention when other platforms were supported for that feature. To determine if a particular feature is supported on your platform, look at the technology configuration guides posted on your product landing page. When a technology configuration guide is displayed on your product landing page, it indicates that the feature is supported on that platform.



CHAPTER 2

Configuring OSPF

This module describes how to configure Open Shortest Path First (OSPF). OSPF is an Interior Gateway Protocol (IGP) developed by the OSPF working group of the Internet Engineering Task Force (IETF). OSPF was designed expressly for IP networks and it supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Cisco supports RFC 1253, *OSPF Version 2 Management Information Base*, August 1991. The OSPF MIB defines an IP routing protocol that provides management information related to OSPF and is supported by Cisco routers.

For protocol-independent features that work with OSPF, see the "Configuring IP Routing Protocol-Independent Features" module.

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.

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

Cisco OSPF Implementation

The Cisco implementation conforms to the OSPF Version 2 specifications detailed in the Internet RFC 2328. The following list outlines key features supported in the Cisco OSPF implementation:

- Stub areas—The definition of stub areas is supported.
- Route redistribution—Routes learned via any IP routing protocol can be redistributed into any other IP routing protocol. At the intradomain level, OSPF can import routes learned via Interior Gateway Routing Protocol (IGRP), Routing Information Protocol (RIP), and Intermediate System-to-Intermediate System (IS-IS). OSPF routes can also be exported into IGRP, RIP, and IS-IS. At the interdomain level, OSPF can import routes learned via Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP). OSPF routes can be exported into EGP and BGP.
- Authentication—Plain text and message-digest algorithm 5 (MD5) authentication among neighboring routers within an area is supported.
- Routing interface parameters—Configurable parameters supported include interface output cost, retransmission interval, interface transmit delay, router priority, router "dead" and hello intervals, and authentication key.
- Virtual links—Virtual links are supported.
- Not-so-stubby area (NSSA)—RFC 3101, which replaces and is backward compatible with RFC 1587.
- OSPF over demand circuit—RFC 1793.

Router Coordination for OSPF

OSPF typically requires coordination among many internal routers: Area Border Routers (ABRs), which are routers connected to multiple areas, and Autonomous System Boundary Routers (ASBRs). At a minimum, OSPF-based routers or access servers can be configured with all default parameter values, no authentication, and interfaces assigned to areas. If you intend to customize your environment, you must ensure coordinated configurations of all routers.

Route Distribution for OSPF

You can specify route redistribution; see the task "Redistribute Routing Information" in the *Network Protocols Configuration Guide, Part 1*, for information on how to configure route redistribution.

The Cisco OSPF implementation allows you to alter certain interface-specific OSPF parameters, as needed. You are not required to alter any of these parameters, but some interface parameters must be consistent across all routers in an attached network. Those parameters are controlled by the **ip ospf hello-interval**, **ip ospf dead-interval**, and **ip ospf authentication-key** interface configuration commands. Therefore, if you do configure any of these parameters, ensure that the configurations for all routers on your network have compatible values.

By default, OSPF classifies different media into the following three types of networks:

- Broadcast networks (Ethernet, Token Ring, and FDDI)
- Nonbroadcast multiaccess (NBMA) networks (Switched Multimegabit Data Service [SMDS], Frame Relay, and X.25)
- Point-to-point networks (High-Level Data Link Control [HDLC] and PPP)

You can configure your network as either a broadcast or an NBMA network.

X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. See the **x25 map** and **frame-relay map** command pages in the *Cisco IOS Wide-Area Networking Command Reference* publication for more detail.

OSPF Network Type

You have the choice of configuring your OSPF network type as either broadcast or NBMA, regardless of the default media type. Using this feature, you can configure broadcast networks as NBMA networks when, for example, you have routers in your network that do not support multicast addressing. You also can configure NBMA networks (such as X.25, Frame Relay, and SMDS) as broadcast networks. This feature saves you from needing to configure neighbors, as described in the "Configuring OSPF for Nonbroadcast Networks"section later in this module.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits (VCs) from every router to every router, that is, a fully meshed network. This is not true in some cases, for example, because of cost constraints or when you have only a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has VCs to both routers. Note that you need not configure neighbors when using this feature.

An OSPF point-to-multipoint interface is defined as a numbered point-to-point interface having one or more neighbors. It creates multiple host routes. An OSPF point-to-multipoint network has the following benefits compared to NBMA and point-to-point networks:

- Point-to-multipoint is easier to configure because it requires no configuration of neighbor commands, it consumes only one IP subnet, and it requires no designated router election.
- It costs less because it does not require a fully meshed topology.
- It is more reliable because it maintains connectivity in the event of VC failure.

On point-to-multipoint broadcast networks, there is no need to specify neighbors. However, you can specify neighbors with the **neighbor** router configuration command, in which case you should specify a cost to that neighbor.

Before the **point-to-multipoint** keyword was added to the **ip ospf network** interface configuration command, some OSPF point-to-multipoint protocol traffic was treated as multicast traffic. Therefore, the **neighbor** router configuration command was not needed for point-to-multipoint interfaces because multicast took care of the traffic. Hello, update, and acknowledgment messages were sent using multicast. In particular, multicast hello messages discovered all neighbors dynamically.

On any point-to-multipoint interface (broadcast or not), the Cisco IOS software assumed that the cost to each neighbor was equal. The cost was configured with the **ip ospf cost** interface configuration command. In reality, the bandwidth to each neighbor is different, so the cost should differ. With this feature, you can configure a separate cost to each neighbor. This feature applies to point-to-multipoint interfaces only.

Because many routers might be attached to an OSPF network, a *designated router* is selected for the network. Special configuration parameters are needed in the designated router selection if broadcast capability is not configured.

These parameters need only be configured in those devices that are themselves eligible to become the designated router or backup designated router (in other words, routers with a nonzero router priority value).

You can specify the following neighbor parameters, as required:

- Priority for a neighboring router
- Nonbroadcast poll interval

On point-to-multipoint, nonbroadcast networks, use the **neighbor** router configuration command to identify neighbors. Assigning a cost to a neighbor is optional.

Prior to Cisco IOS Release 12.0, some customers were using point-to-multipoint on nonbroadcast media (such as classic IP over ATM), so their routers could not dynamically discover their neighbors. This feature allows the **neighbor** router configuration command to be used on point-to-multipoint interfaces.

Area Parameters

Use OSPF Not-So-Stubby Areas (NSSA) feature to simplify administration if you are an Internet service provider (ISP) or a network administrator that must connect a central site that is using OSPF to a remote site that is using a different routing protocol.

Prior to NSSA, the connection between the corporate site border router and the remote router could not be run as an OSPF stub area because routes for the remote site could not be redistributed into the stub area, and two routing protocols needed to be maintained. A simple protocol such as RIP was usually run and handled the redistribution. With NSSA, you can extend OSPF to cover the remote connection by defining the area between the corporate router and the remote router as an NSSA.

As with OSPF stub areas, NSSA areas cannot be injected with distributed routes via Type 5 LSAs. Route redistribution into an NSSA area is possible only with a special type of LSA that is known as Type 7 that can exist only in an NSSA area. An NSSA ASBR generates the Type 7 LSA so that the routes can be redistributed, and an NSSA ABR translates the Type 7 LSA into a Type 5 LSA, which can be flooded throughout the whole OSPF routing domain. Summarization and filtering are supported during the translation.

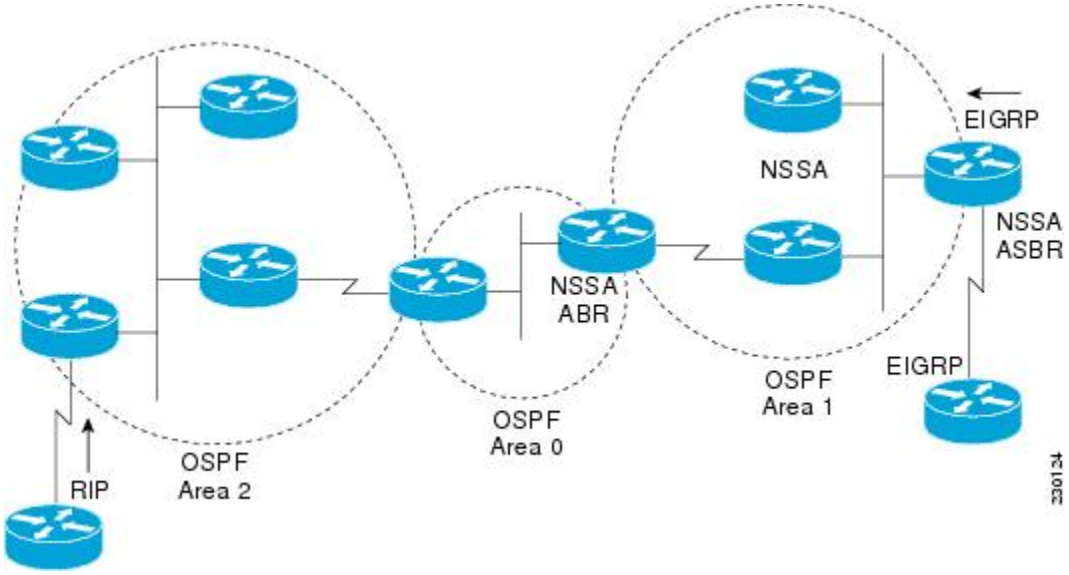
RFC 3101 allows you to configure an NSSA ABR router as a forced NSSA LSA translator. This means that the NSSA ABR router will unconditionally assume the role of LSA translator, preempting the default behavior, which would only include it among the candidates to be elected as translator.

Note Even a forced translator might not translate all LSAs; translation depends on the contents of each LSA.

The figure below shows a network diagram in which OSPF Area 1 is defined as the stub area. The Enhanced Interior Gateway Routing Protocol (EIGRP) routes cannot be propagated into the OSPF domain because

routing redistribution is not allowed in the stub area. However, once OSPF Area 1 is defined as an NSSA, an NSSA ASBR can inject the EIGRP routes into the OSPF NSSA by creating Type 7 LSAs.

Figure 1: OSPF NSSA



The redistributed routes from the RIP router will not be allowed into OSPF Area 1 because NSSA is an extension to the stub area. The stub area characteristics will still exist, including the exclusion of Type 5 LSAs.

Route summarization is the consolidation of advertised addresses. This feature causes a single summary route to be advertised to other areas by an ABR. In OSPF, an ABR will advertise networks in one area into another area. If the network numbers in an area are assigned in a way such that they are contiguous, you can configure the ABR to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

When routes from other protocols are redistributed into OSPF (as described in the module "Configuring IP Routing Protocol-Independent Features"), each route is advertised individually in an external LSA. However, you can configure the Cisco IOS software to advertise a single route for all the redistributed routes that are covered by a specified network address and mask. Doing so helps decrease the size of the OSPF link-state database.

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 two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the nonbackbone area that the two routers have in common (called the transit area). Note that virtual links cannot be configured through stub areas.

You can force an ASBR to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a defaultroute into the OSPF routing domain.

You can configure OSPF to look up Domain Naming System (DNS) names for use in all OSPF show EXEC command displays. You can use this feature to more easily identify a router, because the router is displayed by name rather than by its router ID or neighbor ID.

OSPF uses the largest IP address configured on the interfaces as its router ID. If the interface associated with this IP address is ever brought down, or if the address is removed, the OSPF process must recalculate a new router ID and resend all its routing information out its interfaces.

If a loopback interface is configured with an IP address, the Cisco IOS software will use this IP address as its router ID, even if other interfaces have larger IP addresses. Because loopback interfaces never go down, greater stability in the routing table is achieved.

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 router is chosen. You cannot tell OSPF to use any particular interface.

In Cisco IOS Release 10.3 and later releases, by default OSPF calculates the OSPF metric for an interface according to the bandwidth of the interface. For example, a 64-kbps link gets a metric of 1562, and a T1 link gets a metric of 64.

The OSPF metric is calculated as the ref-bw value divided by the bandwidth value, with the ref-bw value equal to 108 by default, and the bandwidth value determined by the bandwidth interface configuration command. The calculation gives FDDI a metric of 1. If you have multiple links with high bandwidth, you might want to specify a larger number to differentiate the cost on those links.

An administrative distance is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored.

OSPF uses three different administrative distances: intra-area, interarea, and external. Routes within an area are intra-area; routes to another area are interarea; and routes from another routing domain learned via redistribution are external. The default distance for each type of route is 110.

Because simplex interfaces between two devices on an Ethernet represent only one network segment, for OSPF you must configure the sending interface to be a passive interface. This configuration prevents OSPF from sending hello packets for the sending interface. Both devices are able to see each other via the hello packet generated for the receiving interface.

You can configure the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation. You can also configure the hold time between two consecutive SPF calculations.

The OSPF on-demand circuit is an enhancement to the OSPF protocol that allows efficient operation over on-demand circuits such as ISDN, X.25 switched virtual circuits (SVCs), and dialup lines. This feature supports RFC 1793, Extending OSPF to Support Demand Circuits.

Prior to this feature, OSPF periodic hello and LSA updates would be exchanged between routers that connected the on-demand link, even when no changes occurred in the hello or LSA information.

With this feature, periodic hellos are suppressed and the periodic refreshes of LSAs are not flooded over the demand circuit. These packets bring up the link only when they are exchanged for the first time, or when a change occurs in the information they contain. This operation allows the underlying data link layer to be closed when the network topology is stable.

This feature is useful when you want to connect telecommuters or branch offices to an OSPF backbone at a central site. In this case, OSPF for on-demand circuits allows the benefits of OSPF over the entire domain, without excess connection costs. Periodic refreshes of hello updates, LSA updates, and other protocol overhead are prevented from enabling the on-demand circuit when there is no "real" data to send.

Overhead protocols such as hellos and LSAs are transferred over the on-demand circuit only upon initial setup and when they reflect a change in the topology. This means that critical changes to the topology that require new SPF calculations are sent in order to maintain network topology integrity. Periodic refreshes that do not include changes, however, are not sent across the link.

The OSPF LSA group pacing feature allows the router to group OSPF LSAs and pace the refreshing, checksumming, and aging functions. The group pacing results in more efficient use of the router.

The router groups OSPF LSAs and paces the refreshing, checksumming, and aging functions so that sudden increases in CPU usage and network resources are avoided. This feature is most beneficial to large OSPF networks.

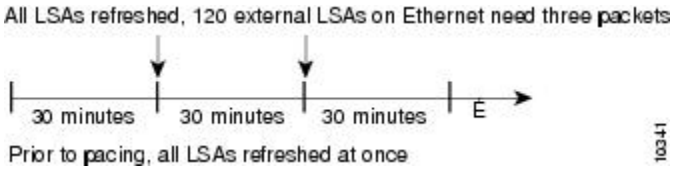
OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

Original LSA Behavior

Each OSPF LSA has an age, which indicates whether the LSA is still valid. Once the LSA reaches the maximum age (1 hour), it is discarded. During the aging process, the originating router sends a refresh packet every 30 minutes to refresh the LSA. Refresh packets are sent to keep the LSA from expiring, whether there has been a change in the network topology or not. Checksumming is performed on all LSAs every 10 minutes. The router keeps track of LSAs that it generates and LSAs that it receives from other routers. The router refreshes LSAs that it generated; it ages the LSAs that it received from other routers.

Prior to the LSA group pacing feature, the Cisco software would perform refreshing on a single timer and checksumming and aging on another timer. In the case of refreshing, for example, the software would scan the whole database every 30 minutes, refreshing every LSA that the router generated, no matter how old it was. The figure below illustrates all the LSAs being refreshed at once. This process wasted CPU resources because only a small portion of the database needed to be refreshed. A large OSPF database (several thousand LSAs) could have thousands of LSAs with different ages. Refreshing on a single timer resulted in the age of all LSAs becoming synchronized, which resulted in much CPU processing at once. Furthermore, a large number of LSAs could cause a sudden increase of network traffic, consuming a large amount of network resources in a short time.

Figure 2: OSPF LSAs on a Single Timer Without Group Pacing



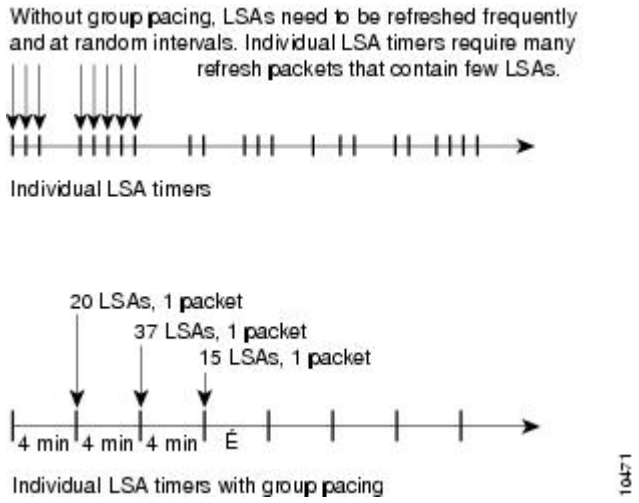
LSA Group Pacing with Multiple Timers

Configuring each LSA to have its own timer avoids excessive CPU processing and sudden network-traffic increase. To again use the example of refreshing, each LSA gets refreshed when it is 30 minutes old, independent of other LSAs. So the CPU is used only when necessary. However, LSAs being refreshed at frequent, random intervals would require many packets for the few refreshed LSAs that the router must send, which would be inefficient use of bandwidth.

Therefore, the router delays the LSA refresh function for an interval of time instead of performing it when the individual timers are reached. The accumulated LSAs constitute a group, which is then refreshed and sent out in one packet or more. Thus, the refresh packets are paced, as are the checksumming and aging. The pacing interval is configurable; it defaults to 4 minutes, which is randomized to further avoid synchronization.

The figure below illustrates the case of refresh packets. The first timeline illustrates individual LSA timers; the second timeline illustrates individual LSA timers with group pacing.

Figure 3: OSPF LSAs on Individual Timers with Group Pacing



The group pacing interval is inversely proportional to the number of LSAs that the router is refreshing, checksumming, and aging. For example, if you have approximately 10,000 LSAs, decreasing the pacing interval would benefit you. If you have a very small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might benefit you slightly.

The default value of pacing between LSA groups is 240 seconds (4 minutes). The range is from 10 seconds to 1800 seconds (30 minutes).

By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives. Some redundancy is desirable, because it ensures robust flooding. However, too much redundancy can waste bandwidth and might destabilize the network due to excessive link and CPU usage in certain topologies. An example would be a fully meshed topology.

You can block OSPF flooding of LSAs in two ways, depending on the type of networks:

- On broadcast, nonbroadcast, and point-to-point networks, you can block flooding over specified OSPF interfaces.
- On point-to-multipoint networks, you can block flooding to a specified neighbor.

The growth of the Internet has increased the importance of scalability in IGPs such as OSPF. By design, OSPF requires LSAs to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to about 50 minutes. This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF flooding reduction solution works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set. The LSAs are now set as “do not age.”

Cisco routers do not support LSA Type 6 Multicast OSPF (MOSPF), and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages.

The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates quickly enough, or the router was out of buffer space. For example, packets might be dropped if either of the following topologies existed:

- A fast router was connected to a slower router over a point-to-point link.
- During flooding, several neighbors sent updates to a single router at the same time.

OSPF update packets are now automatically paced so they are not sent less than 33 milliseconds apart. Pacing is also added between resends to increase efficiency and minimize lost retransmissions. Also, you can display the LSAs waiting to be sent out an interface. The benefit of pacing is that OSPF update and retransmission packets are sent more efficiently. There are no configuration tasks for this feature; it occurs automatically.

You can display specific statistics such as the contents of IP routing tables, caches, and databases. Information provided can be used to determine resource utilization and solve network problems. You can also display information about node reachability and discover the routing path that your device packets are taking through the network.

How to Configure OSPF

To configure OSPF, perform the tasks described in the following sections. The tasks in the "Enabling OSPF" section are required; the tasks in the remaining sections are optional, but might be required for your application. For information about the maximum number of interfaces, see the "Restrictions for OSPF" section.

Enabling OSPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **network** *ip-address wildcard-mask* **area** *area-id*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Device(config-router)# network 192.168.129.16 0.0.0.3 area 20`	Defines an interface on which OSPF runs and defines the area ID for that interface.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF Interface Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf cost** *cost*
5. **ip ospf retransmit-interval** *seconds*
6. **ip ospf transmit-delay** *seconds*
7. **ip ospf priority** *number-value*
8. **ip ospf hello-interval** *seconds*
9. **ip ospf dead-interval** *seconds*
10. **ip ospf authentication-key** *key*
11. **ip ospf message-digest-key** *key-id* **md5** *key*
12. **ip ospf authentication** [**message-digest** | **null**]
13. **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	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf cost** *cost* **Example:** `Device(config-if)# ip ospf cost 65`	Explicitly specifies the cost of sending a packet on an OSPF interface.
Step 5	**ip ospf retransmit-interval** *seconds* **Example:** `Device(config-if)# ip ospf retransmit-interval 1`	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
Step 6	**ip ospf transmit-delay** *seconds* **Example:** `Device(config-if)# ip ospf transmit-delay`	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
Step 7	**ip ospf priority** *number-value* **Example:** `Device(config-if)# ip ospf priority 1`	Sets priority to help determine the OSPF designated router for a network.
Step 8	**ip ospf hello-interval** *seconds* **Example:** `Device(config-if)# ip ospf hello-interval 1`	Specifies the length of time between the hello packets that the Cisco IOS software sends on an OSPF interface.

	Command or Action	Purpose
Step 9	**ip ospf dead-interval** *seconds* **Example:** `Device(config-if)# ip ospf dead-interval 1`	Sets the number of seconds that a device must wait before it declares a neighbor OSPF router down because it has not received a hello packet.
Step 10	**ip ospf authentication-key** *key* **Example:** `Device(config-if)# ip ospf authentication-key 1`	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.
Step 11	**ip ospf message-digest-key** *key-id* **md5** *key* **Example:** `Device(config-if)# ip ospf message-digest-key 1 md5 23456789`	Enables OSPF MD5 authentication. The values for the *key-id* and *key* arguments must match values specified for other neighbors on a network segment.
Step 12	**ip ospf authentication** [**message-digest** | **null**] **Example:** `Device(config-if)# ip ospf authentication message-digest`	Specifies the authentication type for an interface.
Step 13	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring OSPF over Different Physical Networks

Configuring OSPF for Point-to-Multipoint Broadcast Networks

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **ip ospf network point-to-multipoint**
4. **exit**
5. **router ospf** *process-id*
6. **neighbor** *ip-address* [**cost** *number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 3	**ip ospf network point-to-multipoint** **Example:** `Device#(config-if) ip ospf network point-to-multipoint`	Configures an interface as point-to-multipoint for broadcast media.
Step 4	**exit** **Example:** `Device#(config-if) exit`	Enters global configuration mode.
Step 5	**router ospf** *process-id* **Example:** `Device#(config) router ospf 109`	Configures an OSPF routing process and enters router configuration mode.
Step 6	**neighbor** *ip-address* [**cost** *number*] **Example:** `Device#(config-router) neighbor 192.168.3.4 cost 180`	Specifies a neighbor and assigns a cost to the neighbor. **Note** Repeat this step for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the **ip ospf cost** interface configuration command.

Configuring OSPF for Nonbroadcast Networks

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **ip ospf network point-to-multipoint non-broadcast**
4. **exit**
5. **router ospf** *process-id*
6. **neighbor** *ip-address* [**cost** *number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 3	**ip ospf network point-to-multipoint non-broadcast** **Example:** `Device#(config-if) ip ospf network point-to-multipoint non-broadcast`	Configures an interface as point-to-multipoint for nonbroadcast media.
Step 4	**exit** **Example:** `Device#(config-if) exit`	Enters global configuration mode.
Step 5	**router ospf** *process-id* **Example:** `Device#(config) router ospf 109`	Configures an OSPF routing process and enters router configuration mode.
Step 6	**neighbor** *ip-address* [**cost** *number*]	Specifies a neighbor and assigns a cost to the neighbor.

	Command or Action	Purpose
	Example: `Device#(config-router) neighbor 192.168.3.4 cost 180`	**Note** Repeat this step for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the **ip ospf cost** interface configuration command.

Configuring OSPF Area Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **area** *area-id* **authentication**
5. **area** *area-id* **stub** [**no summary**]
6. **area** *area-id* **default-cost** *cost*
7. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.

	Command or Action	Purpose
Step 4	**area** *area-id* **authentication** **Example:** `Device(config-router)# area 10.0.0.0 authentication`	Enables authentication for an OSPF area.
Step 5	**area** *area-id* **stub** [**no summary**] **Example:** `Device(config-router)# area 10.0.0.0 stub no-summary`	Defines an area to be a stub area.
Step 6	**area** *area-id* **default-cost** *cost* **Example:** `Device(config-router)# area 10.0.0.0 default-cost 1`	Specifies a cost for the default summary route that is sent into a stub area or not-so-stubby area (NSSA)
Step 7	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPFv2 NSSA

Configuring an OSPFv2 NSSA Area and Its Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] **[metric** {**metric-value** | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]
5. **network** *ip-address wildcard-mask* **area** *area-id*
6. **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**]
7. **summary-address** *prefix mask* [**not-advertise**] [**tag** *tag*] [**nssa-only**]
8. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. The range is from 1 to 65535.
Step 4	**redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] **[metric** {**metric-value** | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**] **Example:** `Device(config-router)# redistribute rip subnets`	Redistributes routes from one routing domain to another routing domain. • In the example, Routing Information Protocol (RIP) subnets are redistributed into the OSPF domain.
Step 5	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Device(config-router)# network 192.168.129.11 0.0.0.255 area 1`	Defines the interfaces on which OSPF runs and the area ID for those interfaces.
Step 6	**area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric**] [**metric-type**]] [**no-summary**] [**nssa-only**] **Example:** `Device(config-router)# area 1 nssa`	Configures a Not-So-Stubby Area (NSSA) area.
Step 7	**summary-address** *prefix mask* [**not-advertise**] [**tag** *tag*] [**nssa-only**] **Example:** `Device(config-router)# summary-address 10.1.0.0`	Controls the route summarization and filtering during the translation and limits the summary to NSSA areas.

	Command or Action	Purpose
	`255.255.0.0 not-advertise`	
Step 8	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring an NSSA ABR as a Forced NSSA LSA Translator

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **area** *area-id* **nssa translate type7 always**
5. **area** *area-id* **nssa translate type7 suppress-fa**
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 ospf** *process-id* **Example:** `Device(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. The range is from 1 to 65535.

	Command or Action	Purpose
Step 4	**area** *area-id* **nssa translate type7 always** **Example:** `Device(config-router)# area 10 nssa translate type7 always`	Configures a Not-So-Stubby Area Area Border Router (NSSA ABR) device as a forced NSSA Link State Advertisement (LSA) translator. **Note** You can use the **always** keyword in the **area nssa translate** command to configure an NSSA ABR device as a forced NSSA LSA translator. This command can be used if RFC 3101 is disabled and RFC 1587 is used.
Step 5	**area** *area-id* **nssa translate type7 suppress-fa** **Example:** `Device(config-router)# area 10 nssa translate type7 suppress-fa`	Allows ABR to suppress the forwarding address in translated Type-5 LSA.
Step 6	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **compatible rfc1587**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. • Use **router ospf** *process-id* command to enable OSPFv2 routing.
Step 4	**compatible rfc1587** **Example:** `Device(config-router)# compatible rfc1587`	Enables the device to be RFC 1587 compliant.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF NSSA Parameters

Prerequisites

Evaluate the following considerations before you implement this feature:

- You can set a Type 7 default route that can be used to reach external destinations. When configured, the device generates a Type 7 default into the Not-So-Stubby Area (NSSA or the NSSA Area Border Router (ABR).
- Every device within the same area must agree that the area is NSSA; otherwise, the devices cannot communicate.

Configuring Route Summarization Between OSPF Areas

Configuring Route Summarization When Redistributing Routes into OSPF

SUMMARY STEPS

1. **summary-address** {*ip-address mask* | *prefix mask*} [**not-advertise**][**tag** *tag* [**nssa-only**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**summary-address** {*ip-address mask* | *prefix mask*} [**not-advertise**][**tag** *tag* [**nssa-only**] **Example:** `Device#(config-router) summary-address 10.1.0.0 255.255.0.0`	Specifies an address and mask that covers redistributed routes, so that only one summary route is advertised. • You can use the optional **not-advertise** keyword to filter out a set of routes.

Establishing Virtual Links

SUMMARY STEPS

1. **area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**authentication-key** *key* | **message-digest-key** *key-id* **md5** *key*] **Example:** `Device(config-router-af)# area 1 virtual-link 10.1.1.1 router1`	Establishes a virtual link.

Generating a Default Route

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]
5. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*] **Example:** `Device(config-router)# default-information originate always`	Forces the ASBR to generate a default route into the OSPF routing domain. **Note** The **always** keyword includes the following exception when a route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring Lookup of DNS Names

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ospf name-lookup**
4. **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	**ip ospf name-lookup** **Example:** `Device# ip ospf name-lookup`	Enables OSPF routing and enters router configuration mode.
Step 4	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Forcing the Router ID Choice with a Loopback Interface

SUMMARY STEPS

1. **configure terminal**
2. **interface** *type number*
3. **ip address** *ip-address mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface** *type number* **Example:** `Device(config)# interface loopback 0`	Creates a loopback interface and enters interface configuration mode.
Step 3	**ip address** *ip-address mask* **Example:** `Device#(config-if) ip address 192.108.1.27 255.255.255.0`	Assigns an IP address to this interface.

Controlling Default Metrics

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **auto-cost reference-bandwidth** *ref-bw*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**auto-cost reference-bandwidth** *ref-bw* **Example:** `Device(config-router)# auto-cost reference-bandwidth 101`	Differentiates high -bandwidth links.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Changing the OSPF Administrative Distances

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **distance ospf** {**intra-area** | **inter-area** | **external**} *dist*
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**distance ospf** {**intra-area** | **inter-area** | **external**} *dist* **Example:** `Device(config-router)# distance ospf external 200`	Changes the OSPF distance values.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF on Simplex Ethernet Interfaces

Command	Purpose
passive-interface *interface-type interface-number*	Suppresses the sending of hello packets through the specified interface.

Configuring Route Calculation Timers

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **Example:** `Device(config-router)# timers throttle spf 5 1000 9000`	Configures route calculation timers.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF over On-Demand Circuits

SUMMARY STEPS

1. **router ospf** *process-id*
2. **interface** *type number*
3. **ip ospf demand-circuit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**router ospf** *process-id*	Enables OSPF operation.
Step 2	**interface** *type number*	Enters interface configuration mode.
Step 3	**ip ospf demand-circuit**	Configures OSPF over an on-demand circuit.

What to Do Next

Note You can prevent an interface from accepting demand-circuit requests from other routers to by specifying the **ignore** keyword in the **ip ospf demand-circuit** command.

Prerequisites

Evaluate the following considerations before implementing the On-Demand Circuits feature:

- Because LSAs that include topology changes are flooded over an on-demand circuit, we recommend that you put demand circuits within OSPF stub areas or within NSSAs to isolate the demand circuits from as many topology changes as possible.
- Every router within a stub area or NSSA must have this feature loaded in order to take advantage of the on-demand circuit functionality. If this feature is deployed within a regular area, all other regular areas must also support this feature before the demand circuit functionality can take effect because Type 5 external LSAs are flooded throughout all areas.
- Hub-and-spoke network topologies that have a point-to-multipoint (P2MP) OSPF interface type on a hub might not revert to nondemand circuit mode when needed. You must simultaneously reconfigure OSPF on all interfaces on the P2MP segment when reverting them from demand circuit mode to nondemand circuit mode.
- Do not implement this feature on a broadcast-based network topology because the overhead protocols (such as hello and LSA packets) cannot be successfully suppressed, which means the link will remain up.
- Configuring the router for an OSPF on-demand circuit with an asynchronous interface is not a supported configuration. The supported configuration is to use dialer interfaces on both ends of the circuit. For more information, refer to Why OSPF Demand Circuit Keeps Bringing Up the Link .

Logging Neighbors Going Up or Down

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **log-adjacency-changes** [**detail**]
5. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**log-adjacency-changes** [**detail**] **Example:** `Device(config-router)# log-adjacency-changes detail`	Changes the group pacing of LSAs. **Note** Configure the **log-adjacency-changes** command if you want to know about OSPF neighbors going up or down without turning on the **debug ip ospf adjacency** EXEC command because the **log-adjacency-changes** command provides a higher-level view of the peer relationship with less output. Configure the **log-adjacency-changes detail** command if you want to see messages for each state change.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Changing the LSA Group Pacing Interval

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers pacing lsa-group** *seconds*
5. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**timers pacing lsa-group** *seconds* **Example:** `Device(config-router)# timers pacing lsa-group 60`	Changes the group pacing of LSAs.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Blocking OSPF LSA Flooding

Command	Purpose
ip ospf database-filter all out	Blocks the flooding of OSPF LSA packets to the interface.

On point-to-multipoint networks, to block flooding of OSPF LSAs, use the following command in router configuration mode:

Command	Purpose
neighbor *ip-address* **database-filter all out**	Blocks the flooding of OSPF LSA packets to the specified neighbor.

Reducing LSA Flooding

Command	Purpose
ip ospf flood-reduction	Suppresses the unnecessary flooding of LSAs in stable topologies.

Ignoring MOSPF LSA Packets

Command	Purpose
ignore lsa mospf	Prevents the router from generating syslog messages when it receives MOSPF LSA packets.

Monitoring and Maintaining OSPF

Command	Purpose
show ip ospf [*process-id*]	Displays general information about OSPF routing processes.
show ip ospf border-routers	Displays the internal OSPF routing table entries to the ABR and ASBR.
	Displays lists of information related to the OSPF database.

Command	Purpose
show ip ospf [*process-id* [*area-id*]] **database** **show ip ospf** [*process-id* [*area-id*]] **database** [**database-summary**] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [**self-originate**] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [**adv-router** [*ip-address*]] **show ip ospf** [*process-id* [*area-id*]] **database** [**router**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**network**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**summary**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**asbr-summary**] [*link-state-id*] **show ip ospf** [*process-id* [Router# *area-id*]] **database** [**external**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**nssa-external**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-link**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-area**] [*link-state-id*] **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-as**] [*link-state-id*]	
show ip ospf flood-list interface *type*	Displays a list of LSAs waiting to be flooded over an interface (to observe OSPF packet pacing).
show ip ospf interface [*type number*]	Displays OSPF-related interface information.

Command	Purpose
show ip ospf neighbor [*interface-name*] [*neighbor-id*] **detail**	Displays OSPF neighbor information on a per-interface basis.
show ip ospf request-list [*neighbor*] [*interface*] [*interface-neighbor*]	Displays a list of all LSAs requested by a router.
show ip ospf retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	Displays a list of all LSAs waiting to be re-sent.
show ip ospf [*process-id*] **summary-address**	Displays a list of all summary address redistribution information configured under an OSPF process.
show ip ospf virtual-links	Displays OSPF-related virtual links information.

To restart an OSPF process, use the following command in EXEC mode:

Command	Purpose
clear ip ospf [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [**neighbor -** *interface*] [*neighbor-id*]]}	Clears redistribution based on the OSPF routing process ID. If the *pid* option is not specified, all OSPF processes are cleared.

Displaying OSPF Update Packet Pacing

SUMMARY STEPS

1. **show ip ospf flood-list** *interface-type interface-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**show ip ospf flood-list** *interface-type interface-number* **Example:** `Device> show ip ospf flood-list ethernet 1`	Displays a list of OSPF LSAs waiting to be flooded over an interface.

Restrictions for OSPF

On systems with a large number of interfaces, it may be possible to configure OSPF such that the number of links advertised in the router LSA causes the link-state update packet to exceed the size of a "huge" Cisco buffer. To resolve this problem, reduce the number of OSPF links or increase the huge buffer size by entering the **buffers huge size** *size* command.

A link-state update packet containing a router LSA typically has a fixed overhead of 196 bytes, and an additional 12 bytes are required for each link description. With a huge buffer size of 18024 bytes, there can be a maximum of 1485 link descriptions.

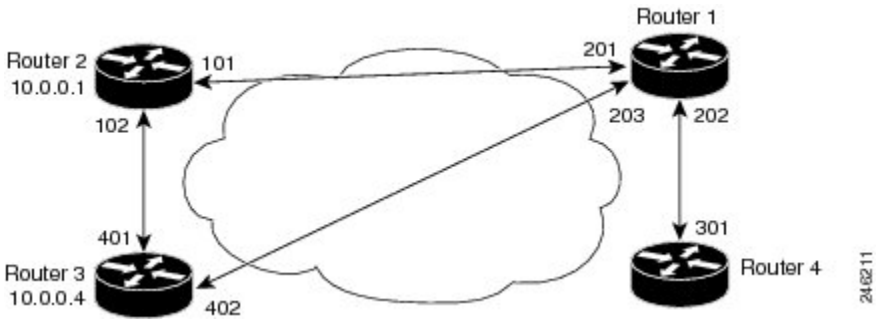
Because the maximum size of an IP packet is 65,535 bytes, there is still an upper bound on the number of links possible on a router.

Configuration Examples for OSPF

Example: OSPF Point-to-Multipoint

In the figure below, Router 1 uses data-link connection identifier (DLCI) 201 to communicate with Router 2, DLCI 202 to communicate with Router 4, and DLCI 203 to communicate with Router 3. Router 2 uses DLCI 101 to communicate with Router 1 and DLCI 102 to communicate with Router 3. Router 3 communicates with Router 2 (DLCI 401) and Router 1 (DLCI 402). Router 4 communicates with Router 1 (DLCI 301). Configuration examples follow the figure.

Figure 4: OSPF Point-to-Multipoint Example



Router 1 Configuration

```
hostname Router 1
!
interface serial 1
 ip address 10.0.0.2 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.1 201 broadcast
 frame-relay map ip 10.0.0.3 202 broadcast
 frame-relay map ip 10.0.0.4 203 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Router 2 Configuration

```
hostname Router 2
!
interface serial 0
 ip address 10.0.0.1 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay map ip 10.0.0.2 101 broadcast
 frame-relay map ip 10.0.0.4 102 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Router 3 Configuration

```
hostname Router 3
!
interface serial 3
 ip address 10.0.0.4 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 1000000
 frame-relay map ip 10.0.0.1 401 broadcast
 frame-relay map ip 10.0.0.2 402 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Router 4 Configuration

```
hostname Router 4
!
interface serial 2
 ip address 10.0.0.3 255.0.0.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 clock rate 2000000
 frame-relay map ip 10.0.0.2 301 broadcast
!
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
```

Example: OSPF Point-to-Multipoint with Broadcast

The following example illustrates a point-to-multipoint network with broadcast:

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 encapsulation frame-relay
 ip ospf cost 100
 ip ospf network point-to-multipoint
 frame-relay map ip 10.0.1.3 202 broadcast
 frame-relay map ip 10.0.1.4 203 broadcast
 frame-relay map ip 10.0.1.5 204 broadcast
 frame-relay local-dlci 200
!
router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
 neighbor 10.0.1.5 cost 5
 neighbor 10.0.1.4 cost 10
```

The following example shows the configuration of the neighbor at 10.0.1.3:

```
interface serial 0
 ip address 10.0.1.3 255.255.255.0
 ip ospf network point-to-multipoint
 encapsulation frame-relay
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300 broadcast
 no shutdown
!
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration is as follows:

```
Device# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/  -        00:01:50    10.0.1.5        Serial0
172.16.1.4        1   FULL/  -        00:01:47    10.0.1.4        Serial0
172.16.1.8        1   FULL/  -        00:01:45    10.0.1.3        Serial0
```

The route information in the first configuration is as follows:

```
Device# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
C    1.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.0.1.3/32 [110/100] via 10.0.1.3, 00:39:08, Serial0
C       10.0.1.0/24 is directly connected, Serial0
O       10.0.1.5/32 [110/5] via 10.0.1.5, 00:39:08, Serial0
O       10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0
```

Example: OSPF Point-to-Multipoint with Nonbroadcast

The following example illustrates a point-to-multipoint network with nonbroadcast:

```
interface Serial0
 ip address 10.0.1.1 255.255.255.0
 ip ospf network point-to-multipoint non-broadcast
 encapsulation frame-relay
 no keepalive
 frame-relay local-dlci 200
 frame-relay map ip 10.0.1.3 202
 frame-relay map ip 10.0.1.4 203
 frame-relay map ip 10.0.1.5 204
 no shutdown
 !
 router ospf 1
  network 10.0.1.0 0.0.0.255 area 0
  neighbor 10.0.1.3 cost 5
  neighbor 10.0.1.4 cost 10
  neighbor 10.0.1.5 cost 15
```

The following example is the configuration for the router on the other side:

```
interface Serial9/2
 ip address 10.0.1.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-multipoint non-broadcast
 no ip mroute-cache
 no keepalive
 no fair-queue
```

```
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300
 no shutdown
 !
 router ospf 1
  network 10.0.1.0 0.0.0.255 area 0
```

The output shown for neighbors in the first configuration is as follows:

```
Device# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.1.1        1   FULL/  -        00:01:52    10.0.1.5        Serial0
172.16.1.4        1   FULL/  -        00:01:52    10.0.1.4        Serial0
172.16.1.8        1   FULL/  -        00:01:52    10.0.1.3        Serial0
```

Example: Variable-Length Subnet Masks

OSPF, static routes, and IS-IS support variable-length subnet masks (VLSMs). With VLSMs, you can use different masks for the same network number on different interfaces, which allows you to conserve IP addresses and more efficiently use available address space.

In the following example, a 30-bit subnet mask is used, leaving two bits of address space reserved for serial-line host addresses. There is sufficient host address space for two host endpoints on a point-to-point serial link.

```
interface ethernet 0
 ip address 172.16.10.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface serial 0
 ip address 172.16.20.1 255.255.255.252
! 2 bits of address space reserved for serial lines
! Router is configured for OSPF and assigned AS 107
router ospf 107
! Specifies network directly connected to the router
 network 172.16.0.0 0.0.255.255 area 0.0.0.0
```

Example: Configuring OSPF NSSA

In the following example, an Open Shortest Path First (OSPF) stub network is configured to include OSPF Area 0 and OSPF Area 1, using five devices. Device 3 is configured as the NSSA Autonomous System Border Router (ASBR). Device 2 configured to be the NSSA Area Border Router (ABR). OSPF Area 1 is defined as a Not-So-Stubby Area (NSSA).

Device 1

```
hostname Device1
!
interface Loopback1
 ip address 10.1.0.1 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface Serial10/0
 description Device2 interface s11/0
 ip address 192.168.10.1 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
```

```
!
router ospf 1
 area 1 nssa
!
end
```

Device 2

```
hostname Device2
!
!
interface Loopback1
 ip address 10.1.0.2 255.255.255.255
!
interface Serial10/0
 description Device1 interface s11/0
 no ip address
 shutdown
 serial restart-delay 0
 no cdp enable
!
interface Serial11/0
 description Device1 interface s10/0
 ip address 192.168.10.2 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
interface Serial14/0
 description Device3 interface s13/0
 ip address 192.168.14.2 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 area 1 nssa
!
end
```

Device 3

```
hostname Device3
!
interface Loopback1
 ip address 10.1.0.3 255.255.255.255
!
interface Ethernet3/0
 ip address 192.168.3.3 255.255.255.0
 no cdp enable
!
interface Serial13/0
 description Device2 interface s14/0
 ip address 192.168.14.3 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
router ospf 1
 log-adjacency-changes
 area 1 nssa
 redistribute rip subnets
!
router rip
 version 2
 redistribute ospf 1 metric 15
 network 192.168.3.0
end
```

Device 4

```
hostname Device4
!
interface Loopback1
 ip address 10.1.0.4 255.255.255.255
!
interface Ethernet3/0
 ip address 192.168.3.4 255.255.255.0
 no cdp enable
!
interface Ethernet4/1
 ip address 192.168.41.4 255.255.255.0
!
router rip
 version 2
 network 192.168.3.0
 network 192.168.41.0
!
end
```

Device 5

```
hostname Device5
!
interface Loopback1
 ip address 10.1.0.5 255.255.255.255
!
interface Ethernet0/0
 ip address 192.168.0.10 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface Ethernet1/1
 ip address 192.168.11.10 255.255.255.0
 ip ospf 1 area 0
!
router ospf 1
!
end
```

Example: OSPF NSSA Area with RFC 3101 Disabled and RFC 1587 Active

In the following example, the output for the **show ip ospf** and **show ip ospf database nssa** commands shows an Open Shortest Path First Not-So-Stubby Area (OSPF NSSA) area where RFC 3101 is disabled, RFC 1587 is active, and an NSSA Area Border Router (ABR) device is configured as a forced NSSA LSA translator. If RFC 3101 is disabled, the forced NSSA LSA translator remains inactive.

```
Device# show ip ospf

Routing Process "ospf 1" with ID 10.0.2.1
Start time: 00:00:25.512, Time elapsed: 00:01:02.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Supports NSSA (compatible with RFC 1587)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
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 0. Checksum Sum 0x000000
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 1. 0 normal 0 stub 1 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area 1
Number of interfaces in this area is 1
It is a NSSA area
Configured to translate Type-7 LSAs, inactive (RFC3101 support
disabled)
Area has no authentication
SPF algorithm last executed 00:00:07.160 ago
SPF algorithm executed 3 times
Area ranges are
Number of LSA 3. Checksum Sum 0x0245F0
Number of opaque link LSA 0. Checksum Sum 0x000000
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

The table below describes the **show ip ospf** display fields and their descriptions.

Table 1: show ip ospf Field Descriptions

Field	Description
Supports NSSA (compatible with RFC 1587)	Specifies that RFC 1587 is active or that the OSPF NSSA area is RFC 1587 compatible.
Configured to translate Type-7 LSAs, inactive (RFC3101 support disabled)	Specifies that OSPF NSSA area has an ABR device configured to act as a forced translator of Type 7 LSAs. However, it is inactive because RFC 3101 is disabled

```
Device2# show ip ospf database nssa

Router Link States (Area 1)
LS age: 28
Options: (No TOS-capability, DC)
LS Type: Router Links
Link State ID: 10.0.2.1
Advertising Router: 10.0.2.1
LS Seq Number: 80000004
Checksum: 0x5CA2
Length: 36
Area Border Router
AS Boundary Router
Unconditional NSSA translator
Number of Links: 1
Link connected to: a Stub Network
(Link ID) Network/subnet number: 192.0.2.5
(Link Data) Network Mask: 255.255.255.0
Number of MTID metrics: 0
TOS 0 Metrics: 10
```

The table below describes the **show ip ospf database nssa** display fields and their descriptions.

Table 2: show ip ospf database nssa Field Descriptions

Field	Description
Unconditional NSSA translator	Specifies that NSSA ASBR device is a forced NSSA LSA translator

Example: OSPF Routing and Route Redistribution

OSPF typically requires coordination among many internal routers, ABRs, and ASBRs. At a minimum, OSPF-based routers can be configured with all default parameter values, with no authentication, and with interfaces assigned to areas.

Three types of examples follow:

- The first is a simple configuration illustrating basic OSPF commands.
- The second example illustrates a configuration for an internal router, ABR, and ASBRs within a single, arbitrarily assigned, OSPF autonomous system.
- The third example illustrates a more complex configuration and the application of various tools available for controlling OSPF-based routing environments.

Example: Basic OSPF Configuration

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches Ethernet interface 0 to area 0.0.0.0, and redistributes RIP into OSPF and OSPF into RIP:

```
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
!
router ospf 9000
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 redistribute rip metric 1 subnets
!
router rip
 network 10.94.0.0
 redistribute ospf 9000
 default-metric 1
```

Example: Basic OSPF Configuration for Internal Router ABR and ASBRs

The following example illustrates the assignment of four area IDs to four IP address ranges. In the example, OSPF routing process 109 is initialized, and four OSPF areas are defined: 10.9.50.0, 2, 3, and 0. Areas 10.9.50.0, 2, and 3 mask specific address ranges, and area 0 enables OSPF for *all other* networks.

```
router ospf 109
 network 192.168.10.0 0.0.0.255 area 10.9.50.0
 network 192.168.20.0 0.0.255.255 area 2
 network 192.168.30.0 0.0.0.255 area 3
 network 192.168.40.0 255.255.255.255 area 0
```

```
!
! Interface Ethernet0 is in area 10.9.50.0:
interface ethernet 0
 ip address 192.168.10.5 255.255.255.0
!
! Interface Ethernet1 is in area 2:
interface ethernet 1
 ip address 192.168.20.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
interface ethernet 2
 ip address 192.168.20.7 255.255.255.0
!
! Interface Ethernet3 is in area 3:
interface ethernet 3
 ip address 192.169.30.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
interface ethernet 4
 ip address 192.168.40.1 255.255.255.0
!
! Interface Ethernet5 is in area 0:
interface ethernet 5
 ip address 192.168.40.12 255.255.0.0
```

Each **network area** router configuration command is evaluated sequentially, so the order of these commands in the configuration is important. The Cisco software sequentially evaluates the address/wildcard-mask pair for each interface. See the **network area** command page in the *Cisco IOS IP Routing: OSPF Command Reference* for more information.

Consider the first **network area** command. Area ID 10.9.50.0 is configured for the interface on which subnet 192.168.10.0 is located. Assume that a match is determined for Ethernet interface 0. Ethernet interface 0 is attached to area 10.9.50.0 only.

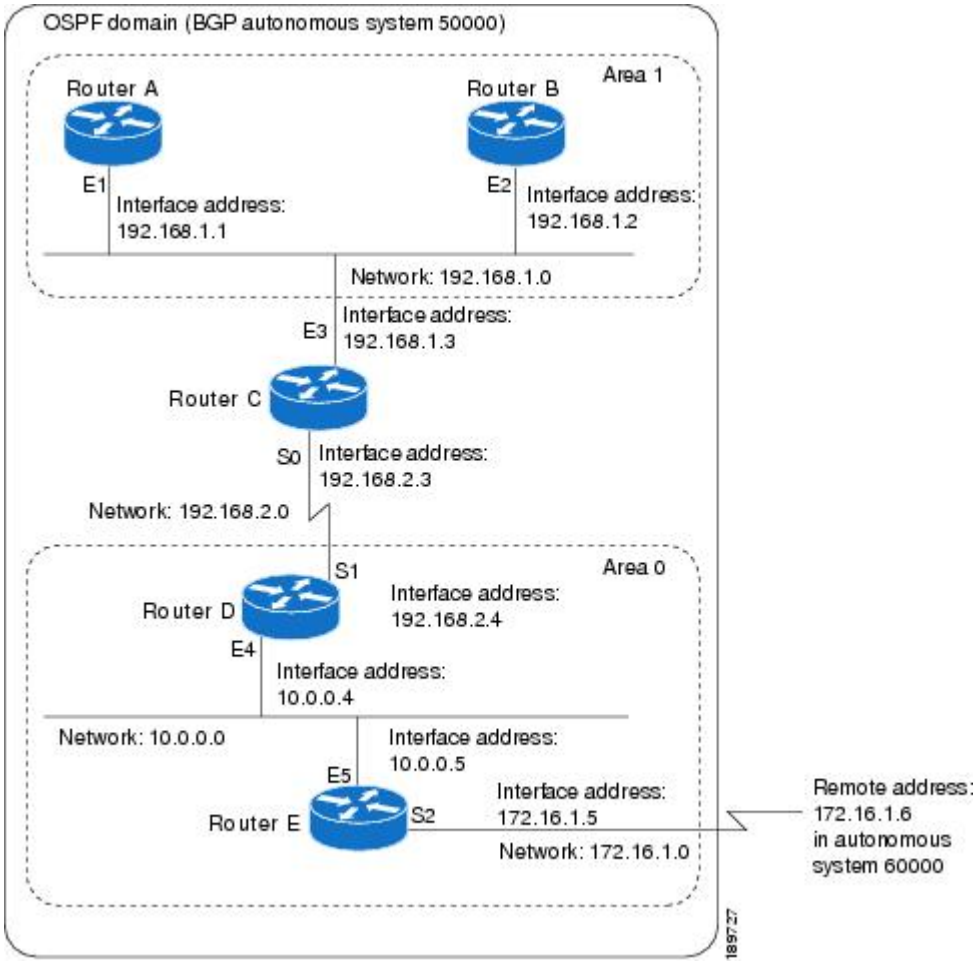
The second **network area** command is evaluated next. For area 2, the same process is then applied to all interfaces (except Ethernet interface 0). Assume that a match is determined for Ethernet interface 1. OSPF is then enabled for that interface, and Ethernet interface 1 is attached to area 2.

This process of attaching interfaces to OSPF areas continues for all **network area** commands. Note that the last **network area** command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to area 0.

Example: Complex Internal Router with ABR and ASBR

The following example outlines a configuration for several routers within a single OSPF autonomous system. The figure below provides a general network map that illustrates this sample configuration.

Figure 5: Sample OSPF Autonomous System Network Map



In this configuration, five routers are configured with OSPF:

- Router A and Router B are both internal routers within area 1.
- Router C is an OSPF ABR. Note that for Router C, Area 1 is assigned to E3 and area 0 is assigned to S0.
- Router D is an internal router in area 0 (backbone area). In this case, both **network** router configuration commands specify the same area (area 0, or the backbone area).
- Router E is an OSPF ASBR. Note that BGP routes are redistributed into OSPF and that these routes are advertised by OSPF.

Note You do not need to include definitions of all areas in an OSPF autonomous system in the configuration of all routers in the autonomous system. Only the *directly* connected areas must be defined. In the example that follows, routes in area 0 are learned by the routers in area 1 (Router A and Router B) when the ABR (Router C) injects summary LSAs into area 1.

The OSPF domain in BGP autonomous system 109 is connected to the outside world via the BGP link to the external peer at IP address 10.0.0.6. Sample configurations follow.

Following is the sample configuration for the general network map shown in the figure above.

Router A Configuration—Internal Router

```
interface ethernet 1
 ip address 192.168.1.1 255.255.255.0
router ospf 1
 network 192.168.0.0 0.0.255.255 area 1
```

Router B Configuration—Internal Router

```
interface ethernet 2
 ip address 192.168.1.2 255.255.255.0
router ospf 202
 network 192.168.0.0 0.0.255.255 area 1
```

Router C Configuration—ABR

```
interface ethernet 3
 ip address 192.168.1.3 255.255.255.0
interface serial 0
 ip address 192.168.2.3 255.255.255.0
router ospf 999
 network 192.168.1.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 0
```

Router D Configuration—Internal Router

```
interface ethernet 4
 ip address 10.0.0.4 255.0.0.0
interface serial 1
 ip address 192.168.2.4 255.255.255.0
router ospf 50
 network 192.168.2.0 0.0.0.255 area 0
 network 10.0.0.0 0.255.255.255 area 0
```

Router E Configuration—ASBR

```
interface ethernet 5
 ip address 10.0.0.5 255.0.0.0
interface serial 2
 ip address 172.16.1.5 255.255.255.0
router ospf 65001
 network 10.0.0.0 0.255.255.255 area 0
 redistribute bgp 109 metric 1 metric-type 1
router bgp 109
 network 192.168.0.0
 network 10.0.0.0
 neighbor 172.16.1.6 remote-as 110
```

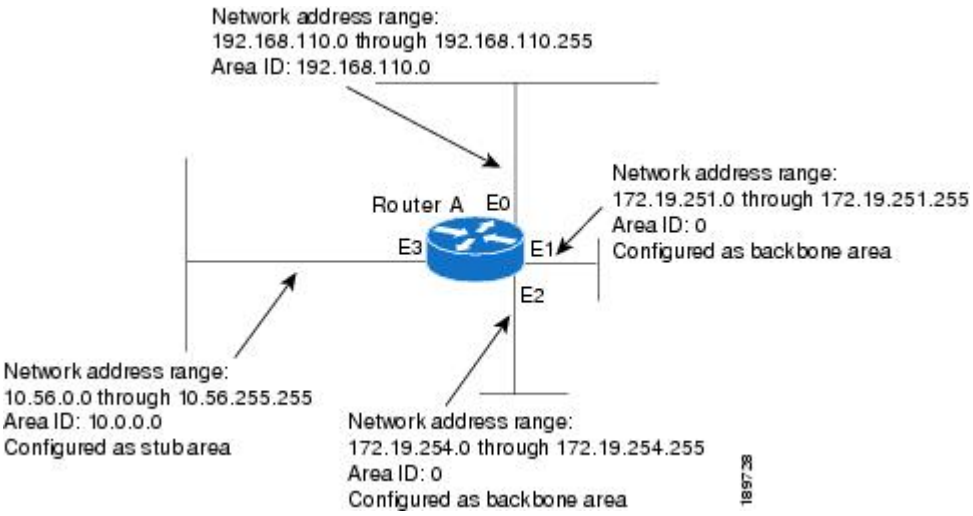
Example: Complex OSPF Configuration for ABR

The following sample configuration accomplishes several tasks in setting up an ABR. These tasks can be split into two general categories:

- Basic OSPF configuration
- Route redistribution

The specific tasks outlined in this configuration are detailed briefly in the following descriptions. The figure below illustrates the network address ranges and area assignments for the interfaces.

Figure 6: Interface and Area Specifications for OSPF Sample Configuration



The basic configuration tasks in this example are as follows:

- Configure address ranges for Ethernet interface 0 through Ethernet interface 3.
- Enable OSPF on each interface.
- Set up an OSPF authentication password for each area and network.
- Assign link-state metrics and other OSPF interface configuration options.
- Create a *stub area* with area ID 36.0.0.0. (Note that the **authentication** and **stub** options of the **area** router configuration command are specified with separate **area** command entries, but can be merged into a single **area** command.)
- Specify the backbone area (area 0).

Configuration tasks associated with redistribution are as follows:

- Redistribute IGRP and RIP into OSPF with various options set (including including **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is a sample OSPF configuration:

```
interface ethernet 0
 ip address 192.0.2.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 1
 ip address 172.19.251.202 255.255.255.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf retransmit-interval 10
 ip ospf transmit-delay 2
 ip ospf priority 4
!
interface ethernet 2
 ip address 172.19.254.2 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface ethernet 3
 ip address 10.56.0.0 255.255.0.0
 ip ospf authentication-key ijklmnop
 ip ospf cost 20
 ip ospf dead-interval 80
```

In the following configuration, OSPF is on network 172.16.0.0:

```
router ospf 201
 network 10.10.0.0 0.255.255.255 area 10.10.0.0
 network 192.42.110.0 0.0.0.255 area 192.42.110.0
 network 172.16.0.0 0.0.255.255 area 0
 area 0 authentication
 area 10.10.0.0 stub
 area 10.10.0.0 authentication
 area 10.10.0.0 default-cost 20
 area 192.42.110.0 authentication
 area 10.10.0.0 range 10.10.0.0 255.0.0.0
 area 192.42.110.0 range 192.42.110.0 255.255.255.0
 area 0 range 172.16.251.0 255.255.255.0
 area 0 range 172.16.254.0 255.255.255.0
 redistribute igrp 200 metric-type 2 metric 1 tag 200 subnets
 redistribute rip metric-type 2 metric 1 tag 200
```

In the following configuration, IGRP autonomous system 200 is on 192.0.2.1:

```
router igrp 200
 network 172.31.0.0
!
! RIP for 192.168.110
!
router rip
 network 192.168.110.0
 redistribute igrp 200 metric 1
 redistribute ospf 201 metric 1
```

Examples: Route Map

The examples in this section illustrate the use of redistribution, with and without route maps. Examples from the IP and Connectionless Network Service (CLNS) routing protocols are given.

The following example redistributes all OSPF routes into IGRP:

```
router igrp 109
 redistribute ospf 110
```

The following example redistributes RIP routes with a hop count equal to 1 into OSPF. These routes will be redistributed into OSPF as external LSAs with a metric of 5, a metric type of Type 1, and a tag equal to 1.

```
router ospf 109
 redistribute rip route-map rip-to-ospf
!
route-map rip-to-ospf permit
 match metric 1
 set metric 5
 set metric-type type1
 set tag 1
```

The following example redistributes OSPF learned routes with tag 7 as a RIP metric of 15:

```
router rip
 redistribute ospf 109 route-map 5
!
route-map 5 permit
 match tag 7
 set metric 15
```

The following example redistributes OSPF intra-area and interarea routes with next-hop routers on serial interface 0 into BGP with an INTER_AS metric of 5:

```
router bgp 109
 redistribute ospf 109 route-map 10
!
route-map 10 permit
 match route-type internal
 match interface serial 0
 set metric 5
```

The following example redistributes two types of routes into the integrated IS-IS routing table (supporting both IP and CLNS). The first type is OSPF external IP routes with tag 5; these routes are inserted into Level 2 IS-IS link state packets (LSPs) with a metric of 5. The second type is ISO-IGRP derived CLNS prefix routes that match CLNS access list 2000; these routes will be redistributed into IS-IS as Level 2 LSPs with a metric of 30.

```
router isis
 redistribute ospf 109 route-map 2
 redistribute iso-igrp nsfnet route-map 3
!
route-map 2 permit
 match route-type external
 match tag 5
 set metric 5
 set level level-2
!
route-map 3 permit
 match address 2000
 set metric 30
```

With the following configuration, OSPF external routes with tags 1, 2, 3, and 5 are redistributed into RIP with metrics of 1, 1, 5, and 5, respectively. The OSPF routes with a tag of 4 are not redistributed.

```
router rip
 redistribute ospf 109 route-map 1
!
route-map 1 permit
 match tag 1 2
 set metric 1
!
route-map 1 permit
 match tag 3
 set metric 5
!
route-map 1 deny
 match tag 4
!
```

```
route map 1 permit
 match tag 5
 set metric 5
```

In the following configuration, a RIP-learned route for network 192.168.0.0 and an ISO-IGRP-learned route with prefix 49.0001.0002 are redistributed into an IS-IS Level 2 LSP with a metric of 5:

```
router isis
 redistribute rip route-map 1
 redistribute iso-igrp remote route-map 1
!
route-map 1 permit
 match ip address 1
 match clns address 2
 set metric 5
 set level level-2
!
 access-list 1 permit 192.168.0.0 0.0.255.255
 clns filter-set 2 permit 49.0001.0002...
```

The following configuration example illustrates how a route map is referenced by the **default-information** router configuration command. This type of reference is called *conditional default origination*. OSPF will originate the default route (network 0.0.0.0) with a Type 2 metric of 5 if 172.16.0.0 is in the routing table.

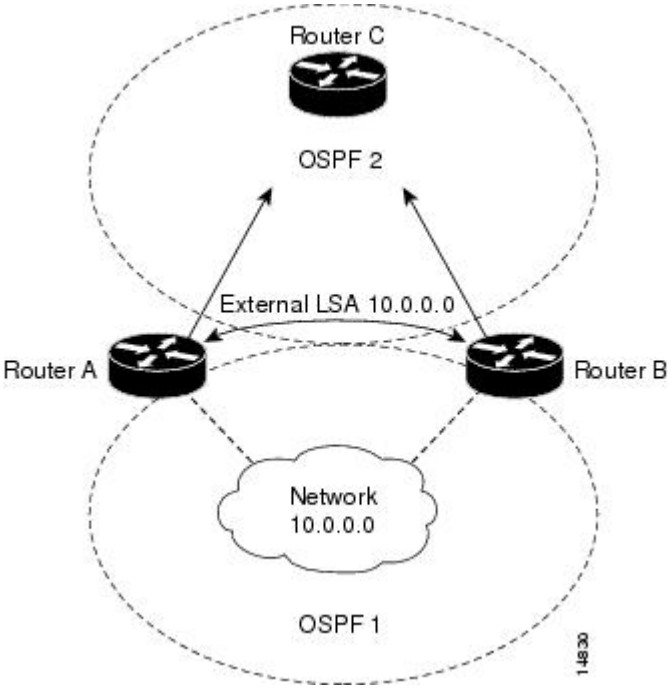
Note Only routes external to the OSPF process can be used for tracking, such as non-OSPF routes or OSPF routes from a separate OSPF process.

```
route-map ospf-default permit
 match ip address 1
 set metric 5
 set metric-type type-2
!
 access-list 1 permit 172.16.0.0 0.0.255.255
!
router ospf 109
 default-information originate route-map ospf-default
```

Example: Changing the OSPF Administrative Distances

The following configuration changes the external distance to 200, making it less trustworthy. The figure below illustrates the example.

Figure 7: OSPF Administrative Distance



Router A Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Router B Configuration

```
router ospf 1
 redistribute ospf 2 subnet
 distance ospf external 200
!
router ospf 2
 redistribute ospf 1 subnet
 distance ospf external 200
```

Example: OSPF over On-Demand Routing

The following configuration allows OSPF over an on-demand circuit, as shown in the figure below. Note that the on-demand circuit is defined on one side only (BRI 0 on Router A); it is not required to be configured on both sides.

Figure 8: OSPF over On-Demand Circuit

Router A Configuration

```
username RouterB password 7 060C1A2F47
isdn switch-type basic-5ess
ip routing
!
interface TokenRing0
 ip address 192.168.50.5 255.255.255.0
 no shutdown
!
interface BRI0
 no cdp enable
 description connected PBX 1485
 ip address 192.168.45.30 255.255.255.0
 encapsulation ppp
 ip ospf demand-circuit
 dialer map ip 192.0.2.6 name RouterB broadcast 61484
 dialer-group 1
 ppp authentication chap
 no shutdown
!
router ospf 100
 network 192.168.45.0 0.0.0.255 area 0
 network 192.168.45.50 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

Router B Configuration

```
username RouterA password 7 04511E0804
isdn switch-type basic-5ess
ip routing
!
interface Ethernet0
 ip address 192.168.50.16 255.255.255.0
 no shutdown
!
interface BRI0
 no cdp enable
 description connected PBX 1484
 ip address  192.168.45.17 255.255.255.0
 encapsulation ppp
 dialer map ip 192.168.45.19 name RouterA broadcast 61485
 dialer-group 1
 ppp authentication chap
 no shutdown
!
router ospf 100
 network 192.168.45.0 0.0.0.255 area 0
```

```
 network 192.168.45.50 0.0.0.255 area 0
!
dialer-list 1 protocol ip permit
```

Example: LSA Group Pacing

The following example changes the OSPF pacing between LSA groups to 60 seconds:

```
router ospf
 timers pacing lsa-group 60
```

Example: Blocking OSPF LSA Flooding

The following example prevents flooding of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
interface ethernet 0
 ip ospf database-filter all out
```

The following example prevents flooding of OSPF LSAs to point-to-multipoint networks to the neighbor at IP address 10.10.10.45:

```
router ospf 109
 neighbor 10.10.10.45 database-filter all out
```

Example: Ignoring MOSPF LSA Packets

The following example configures the router to suppress the sending of syslog messages when it receives MOSPF packets:

```
router ospf 109
 ignore lsa mospf
```

Additional References for OSPF Not-So-Stubby Areas (NSSA)

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Protocol-independent features that work with OSPF	"Configuring IP Routing Protocol-Independent Features" module in *IP Routing: Protocol-Independent Configuration Guide*

RFCs

RFC	Title
RFC 1587	The OSPF NSSA Option, March 1994
RFC 3101	The OSPF NSSA Option January 2003

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

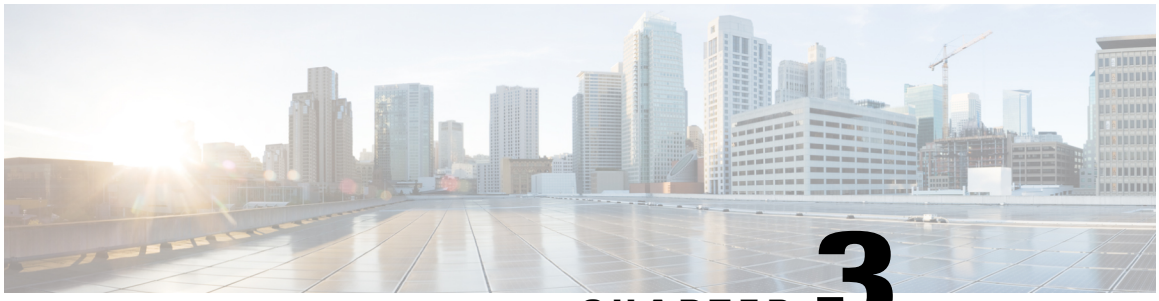
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train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

Feature Name	Releases	Feature Information
OSPF		OSPF is an IGP developed by the OSPF working group of the IETF. Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.

Feature Name	Releases	Feature Information
OSPFv3 RFC 3101 Support	Cisco IOS XE Release 3.7S	The **area nssa translate** (OSPFv3), **compatible rfc1587** (OSPFv3), and **show ospfv3** commands were added. The **nssa-only** keyword was added to the **summary-prefix** (OSPFv3) command.



CHAPTER 3

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.

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.

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.

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. **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*]
7. **ignore lsa mospf**
8. **interface-id snmp-if-index**
9. **log-adjacency-changes** [**detail**]
10. **passive-interface** [**default** | *interface-type interface-number*]
11. **queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**}
12. **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.

	Command or Action	Purpose
Step 4	**area** *area-ID* [**default-cost** | **nssa** | **stub**] **Example:** `Device(config-router)# area 1`	Configures the OSPFv3 area.
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	**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 7	**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 8	**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 9	**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 10	**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 11	**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 12	**router-id** *router-id* **Example:** `Device(config-router)# router-id 10.1.1.1`	Enter this command to use a fixed router ID.

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**	Resets an OSPFv3 process.

	Command or Action	Purpose
	Example: `Device# clear ospfv3 2 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. • 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** **Example:** `Device> enable`	Enables privileged EXEC mode. • 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**	Displays lists of information related to the OSPFv3 database for a specific device.

	Command or Action	Purpose
	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`	
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.
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.

	Command or Action	Purpose
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 statistic`	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: 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

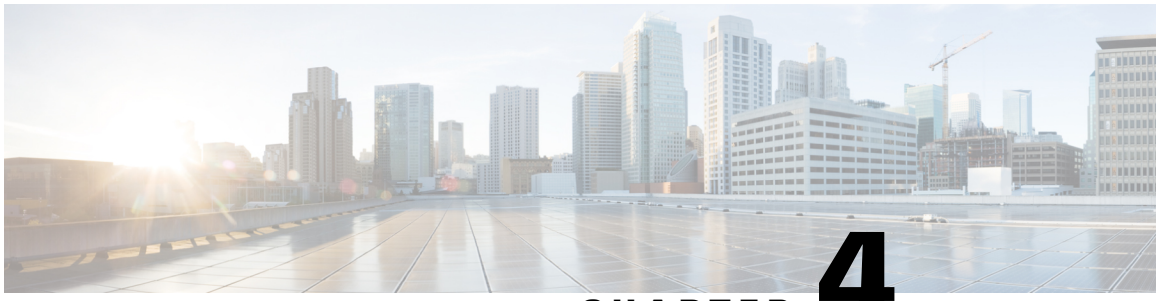
Feature Information for IPv6 Routing: OSPFv3

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 4: Feature Information for IPv6 Routing: OSPFv3

Feature Name	Releases	Feature Information
IPv6 Routing: OSPFv3	12.2(33)SRA 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.



CHAPTER 4

IPv6 Routing: OSPFv3 Authentication Support with IPsec

In order to ensure that Open Shortest Path First version 3 (OSPFv3) packets are not altered and re-sent to the device, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

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.

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 Authentication Support with IPsec

Configure the IP Security (IPsec) secure socket application program interface (API) on OSPFv3 in order to enable authentication and encryption.

Information About IPv6 Routing: OSPFv3 Authentication Support with IPsec

OSPFv3 Authentication Support with IPsec

In order to ensure that OSPFv3 packets are not altered and re-sent to the device, causing the device to behave in a way not desired by its system administrators, OSPFv3 packets must be authenticated. OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. This API supports IPv6.

OSPFv3 requires the use of IPsec to enable authentication. Crypto images are required to use authentication, because only crypto images include the IPsec API needed for use with OSPFv3.

In OSPFv3, authentication fields have been removed from OSPFv3 packet headers. When OSPFv3 runs on IPv6, OSPFv3 requires the IPv6 authentication header (AH) or IPv6 ESP header to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH and ESP extension headers can be used to provide authentication and confidentiality to OSPFv3.

To use the IPsec AH, you must enable the **ipv6 ospf authentication** command. To use the IPsec ESP header, you must enable the **ipv6 ospf encryption** command. The ESP header may be applied alone or in combination with the AH, and when ESP is used, both encryption and authentication are provided. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host.

To configure IPsec, you configure a security policy, which is a combination of the security policy index (SPI) and the key (the key is used to create and validate the hash value). IPsec for OSPFv3 can be configured on an interface or on an OSPFv3 area. For higher security, you should configure a different policy on each interface configured with IPsec. If you configure IPsec for an OSPFv3 area, the policy is applied to all of the interfaces in that area, except for the interfaces that have IPsec configured directly. Once IPsec is configured for OSPFv3, IPsec is invisible to you.

The secure socket API is used by applications to secure traffic. The API needs to allow the application to open, listen, and close secure sockets. The binding between the application and the secure socket layer also allows the secure socket layer to inform the application of changes to the socket, such as connection open and close events. The secure socket API is able to identify the socket; that is, it can identify the local and remote addresses, masks, ports, and protocol that carry the traffic requiring security.

Each interface has a secure socket state, which can be one of the following:

- NULL: Do not create a secure socket for the interface if authentication is configured for the area.
- DOWN: IPsec has been configured for the interface (or the area that contains the interface), but OSPFv3 either has not requested IPsec to create a secure socket for this interface, or there is an error condition.
- GOING UP: OSPFv3 has requested a secure socket from IPsec and is waiting for a CRYPTO_SS_SOCKET_UP message from IPsec.
- UP: OSPFv3 has received a CRYPTO_SS_SOCKET_UP message from IPsec.
- CLOSING: The secure socket for the interface has been closed. A new socket may be opened for the interface, in which case the current secure socket makes the transition to the DOWN state. Otherwise, the interface will become UNCONFIGURED.
- UNCONFIGURED: Authentication is not configured on the interface.

OSPFv3 will not send or accept packets while in the DOWN state.

How to Configure IPv6 Routing: OSPFv3 Authentication Support with IPsec

Configuring IPsec on OSPFv3

Once you have configured OSPFv3 and decided on your authentication, you must define the security policy on each of the devices within the group. The security policy consists of the combination of the key and the SPI. To define a security policy, you must define an SPI and a key.

You can configure an authentication or encryption policy either on an interface or for an OSPFv3 area. When you configure for an area, the security policy is applied to all of the interfaces in the area. For higher security, use a different policy on each interface.

You can configure authentication and encryption on virtual links.

Defining Authentication on an Interface

Before You Begin

Before you configure IPsec on an interface, you must configure OSPFv3 on that interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**} { *key-encryption-type key*} | **null**
   - **ipv6 ospf authentication** {**null** | **ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] [*key*]}

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode. **Note** For Cisco ASR 901 Series Routers, you should configure the OSPFv3 authentication of the VLAN interface, instead of the physical interface. See the below example: `Device(config)# interface VLAN 60`

Step 4	Do one of the following:
	• **ospfv3 authentication** {**ipsec** *spi*} {**md5** | **sha1**}{ *key-encryption-type key*} | **null**
	• **ipv6 ospf authentication** {**null** | **ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] [*key*]}
	
	Example:
	`Device(config-if)# ospfv3 authentication md5 0 27576134094768132473302031209727`
	
	Example:
	Or
	
	`Device(config-if)# ipv6 ospf authentication ipsec spi 500 md5 1234567890abcdef1234567890abcdef`
		Specifies the authentication type for an interface.

Defining Authentication in an OSPFv3 Area

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key*

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	**ipv6 router ospf** *process-id* **Example:** `Device(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**area** *area-id* **authentication ipsec spi** *spi authentication-algorithm* [*key-encryption-type*] *key* **Example:** `Device(config-rtr)# area 1 authentication ipsec spi 678 md5 1234567890ABCDEF1234567890ABCDEF`	Enables authentication in an OSPFv3 area.

Configuration Examples for IPv6 Routing: OSPFv3 Authentication Support with IPsec

Example: Defining Authentication on an Interface

The following example shows how to define authentication on Ethernet interface 0/0:

```
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf 1 area 0
 ipv6 ospf authentication ipsec spi 500 md5 1234567890ABCDEF1234567890ABCDEF
interface Ethernet0/0
 ipv6 enable
 ipv6 ospf authentication null
 ipv6 ospf 1 area 0
```

The following example shows how to define authentication on a VLAN interface of the Cisco ASR 901 Series Router:

```
interface Vlan60
ipv6 ospf encryption ipsec spi 300 esp 3des 4D92199549E0F2EF009B4160F3580E5528A11A45017F3887
 md5 79054025245FB1A26E4BC422AEF54501
```

Example: Defining Authentication in an OSPFv3 Area

The following example shows how to define authentication on OSPFv3 area 0:

```
ipv6 router ospf 1
 router-id 10.11.11.1
 area 0 authentication ipsec spi 1000 md5 1234567890ABCDEF1234567890ABCDEF
```

Additional References for IPv6 Routing: OSPFv3 Authentication Support with IPsec

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: OSPF for IPv6 Authentication Support with IPsec	"*Configuring OSPF*" module in *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	IPv6 RFCs

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

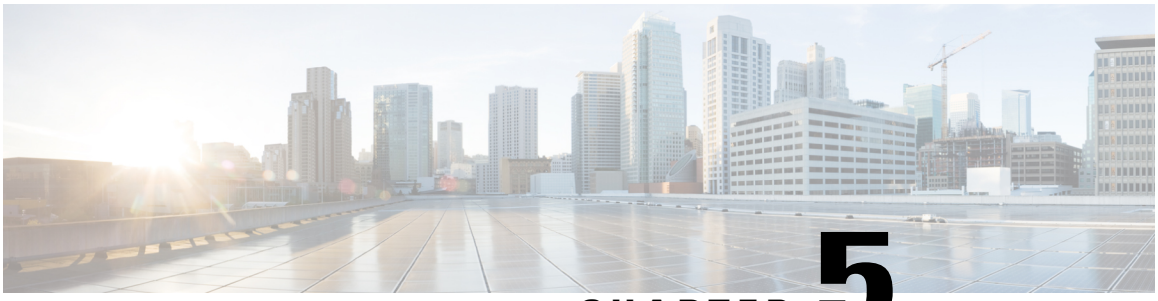
Feature Information for IPv6 Routing: OSPFv3 Authentication Support with IPsec

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 IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec

Feature Name	Releases	Feature Information
IPv6 Routing: OSPF for IPv6 Authentication Support with IPsec	XE 3.14S	OSPFv3 uses the IPsec secure socket API to add authentication to OSPFv3 packets. The following commands were introduced or modified: **area authentication (IPv6)**, **ipv6 ospf authentication**, **ipv6 router ospf**, **ospfv3 authentication**.



CHAPTER 5

OSPFv2 Cryptographic Authentication

To prevent unauthorized or invalid routing updates in your network, Open Shortest Path First version 2 (OSPFv2) protocol packets must be authenticated.

There are two methods of authentication that are defined for OSPFv2: plain text authentication and cryptographic authentication. This module describes how to configure cryptographic authentication using the Hashed Message Authentication Code - Secure Hash Algorithm (HMAC-SHA). OSPFv2 specification (RFC 2328) allows only the Message-Digest 5 (MD5) algorithm for cryptographic authentication. However, RFC 5709 (OSPFv2 HMAC-SHA Cryptographic Authentication) allows OSPFv2 to use HMAC-SHA algorithms for cryptographic authentication.

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.

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 Cryptographic Authentication

Ensure that Open Shortest Path First version 2 (OSPFv2) is configured on your network.

Information About OSPFv2 Cryptographic Authentication

Configuring OSPFv2 Cryptographic Authentication

The OSPFv2 Cryptographic Authentication feature allows you to configure a key chain on the OSPF interface to authenticate OSPFv2 packets by using HMAC-SHA algorithms. You can use an existing key chain that is being used by another protocol, or you can create a key chain specifically for OSPFv2.

A key chain is a list of keys. Each key consists of a key string, which is also called the password or passcode. A key-string is essential for a key to be operational. Each key is identified by a unique key ID. To authenticate the OSPFv2 packets, it is essential that the cryptographic authentication algorithm be configured with a key. OSPFv2 supports keys with key IDs ranging from 1 to 255. The combination of the cryptographic authentication algorithm and the key is known as a Security Association (SA).

The authentication key on a key chain is valid for a specific time period called lifetime. An SA has the following configurable lifetimes:

- Accept lifetime
- Send lifetime

While adding a new key, the Send lifetime is set to a time in the future so that the same key can be configured on all devices in the network before the new key becomes operational. Old keys are removed only after the new key is operational on all devices in the network. When packets are received, the key ID is used to fetch the data for that key. The packet is verified using the cryptographic authentication algorithm and the configured key ID. If the key ID is not found, the packet is dropped.

Use the **ip ospf authentication key-chain** command to configure key chains for OSPFv2 cryptographic authentication.

Note If OSPFv2 is configured to use a key chain, all MD5 keys that were previously configured using the **ip ospf message-digest-key** command are ignored.

How to Configure OSPFv2 Cryptographic Authentication

Defining a Key Chain

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name*
4. **key** *key-id*
5. **key-string** *name*
6. **cryptographic-algorithm** *name*
7. **send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
8. **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	**key chain** *name* **Example:** `Device(config)# key chain sample1`	Specifies the key chain name and enters key-chain configuration mode.
Step 4	**key** *key-id* **Example:** `Device(config-keychain)# key 1`	Specifies the key identifier and enters key-chain key configuration mode. The range is from 1 to 255.

	Command or Action	Purpose
Step 5	**key-string** *name* **Example:** `Device(config-keychain-key)# key-string string1`	Specifies the key string.
Step 6	**cryptographic-algorithm** *name* **Example:** `Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256`	Configures the key with the specified cryptographic algorithm.
Step 7	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*} **Example:** `Device(config-keychain-key)# send-lifetime local 10:00:00 5 July 2013 infinite`	Sets the time period during which an authentication key on a key chain is valid to be sent during key exchange with another device.
Step 8	**end** **Example:** `Device(config-keychain-key)# end`	Exits key-chain key configuration mode and returns to privileged EXEC mode.

Defining Authentication on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf authentication key-chain** *name*
5. **end**

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	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet0/0/0`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**ip ospf authentication key-chain** *name* **Example:** `Device(config-if)# ip ospf authentication key-chain ospf1`	Specifies the key chain for an interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv2 Cryptographic Authentication

Example: Defining a Key Chain

The following example shows how to configure a key chain:

```
Device> enable
Device# configure terminal
Device(config)# key chain sample1
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASampleKey12345
Device(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Device(config-keychain-key)# send-lifetime local 10:00:00 5 July 2013 infinite
Device(config-keychain-key)# end
```

Example: Verifying a Key Chain

The following sample output from the **show key chain** command displays the key chain information:

```
Device# show key chain Key-chain sample1

     key 1 -- text "ThisIsASampleKey12345"
         accept lifetime (always valid) - (always valid) [valid now]
         send lifetime (10:00:00 PDT Jul 5 2013) - (infinite)
```

The table below describes the significant fields in the output:

Table 6: show ip ospf interface Field Descriptions

Field	Description
key	Status of the configured key.
accept lifetime	The time interval within which the device accepts the key during key exchange with another device.
send lifetime	The time interval within which the device sends the key during a key exchange with another device.

Example: Defining Authentication on an Interface

The following example shows how to define authentication on Gigabit Ethernet interface 0/0/0:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet0/0/0
Device (config-if)# ip ospf authentication key-chain sample1
Device (config-if)# end
```

Example: Verifying Authentication on an Interface

The following sample output of the **show ip ospf interface** command displays the cryptographic key information:

```
Device# show ip ospf interface GigabitEthernet0/0/0

GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.8.2/24, Area 1, Attached via Interface Enable
  Process ID 1, Router ID 10.1.1.8, Network Type BROADCAST, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 10.1.1.8, Interface address 192.168.8.2
  Backup Designated router (ID) 10.1.1.9, Interface address 192.168.8.9
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
```

```
Can be protected by per-prefix Loop-Free FastReroute
Can be used for per-prefix Loop-Free FastReroute repair paths
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, 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 10.1.1.9  (Backup Designated Router)
Suppress hello for 0 neighbor(s)
Cryptographic authentication enabled
  Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain sample1
```

The table below describes the significant fields in the output:

Table 7: show ip ospf interface Field Descriptions

Field	Description
GigabitEthernet	Status of the physical link and operational status of the protocol.
Internet Address	Interface IP address, subnet mask, and area address.
Area	OSPF area.
Process ID	OSPF process ID.
Cost	Administrative cost assigned to the interface.
Topology-MTID	MTR topology Multitopology Identifier (MTID) is a number assigned so that the protocol can identify the topology associated with information that it sends to its peers.
Transmit Delay	Transmit delay (in seconds), interface state, and router priority.
State	Operational state of the interface.
Designated Router	Designated router ID and respective interface IP address.
Backup Designated router	Backup designated router ID and respective interface IP address.
Timer intervals configured	Configuration of timer intervals.
Neighbor Count	Count of network neighbors and list of adjacent neighbors.
Cryptographic authentication	Status of cryptographic authentication.
Sending SA	Status of the sending SA (Security Association). Key, cryptographic algorithm, and key chain used.

Additional References for OSPFv2 Cryptographic Authentication

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference

Standards and RFCs

Standard	Title
RFC 2328	OSPF Version 2, April 1998
RFC 5709	OSPFv2 HMAC-SHA Cryptographic Authentication, October 2009

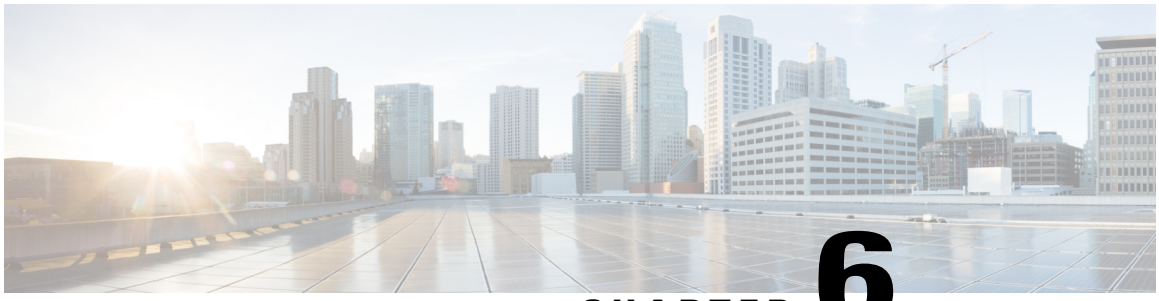
Technical Assistance

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 Cryptographic Authentication

Table 8: Feature Information for OSPFv2 Cryptographic Authentication

Feature Name	Releases	Feature Information
OSPFv2 Cryptographic Authentication	15.4(1)T	The OSPFv2 Cryptographic Authentication feature prevents unauthorized or invalid routing updates in your network by authenticating Open Shortest Path First version 2 (OSPFv2) protocol packets using HMAC-SHA algorithms. The following command was modified: **ip ospf authentication**.



CHAPTER 6

OSPFv3 External Path Preference Option

The Open Shortest Path First version 3 (OSPFv3) external path preference option feature provides a way to calculate external path preferences per RFC 5340.

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.

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 OSPFv3 External Path Preference Option

OSPFv3 External Path Preference Option

Per RFC 5340, the following rules indicate which paths are preferred when multiple intra-AS paths are available to ASBRs or forwarding addresses:

- Intra-area paths using nonbackbone areas are always the most preferred.
- The other paths, intraarea backbone paths and interarea paths, are of equal preference.

These rules apply when the same ASBR is reachable through multiple areas, or when trying to decide which of several AS-external-LSAs should be preferred. In the former case the paths all terminate at the same ASBR, and in the latter the paths terminate at separate ASBRs or forwarding addresses. In either case, each path is represented by a separate routing table entry. This feature applies only when RFC 1583 compatibility is set to disabled using the **no compatibility rfc1583** command (RFC 5340 provides an update to RFC 1583).

Caution To minimize the chance of routing loops, set identical RFC compatibility for all OSPF routers in an OSPF routing domain.

How to Calculate OSPFv3 External Path Preference Option

Calculating OSPFv3 External Path Preferences per RFC 5340

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **no compatible rfc1583**

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 OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

	Command or Action	Purpose
Step 4	**no compatible rfc1583** **Example:** `Device(config-router)# no compatible rfc1583`	Changes the method used to calculate external path preferences per RFC 5340.

Configuration Examples for OSPFv3 External Path Preference Option

Example: Calculating OSPFv3 External Path Preferences per RFC 5340

```
show ospfv3

Routing Process "ospfv3 1" with ID 10.1.1.1
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Reference bandwidth unit is 100 mbps
 RFC 1583 compatibility disabled
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        SPF algorithm executed 1 times
        Number of LSA 1. Checksum Sum 0x00D03D
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

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

Related Topic	Document Title
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping
OSPFv3 External Path Preference Option	*"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

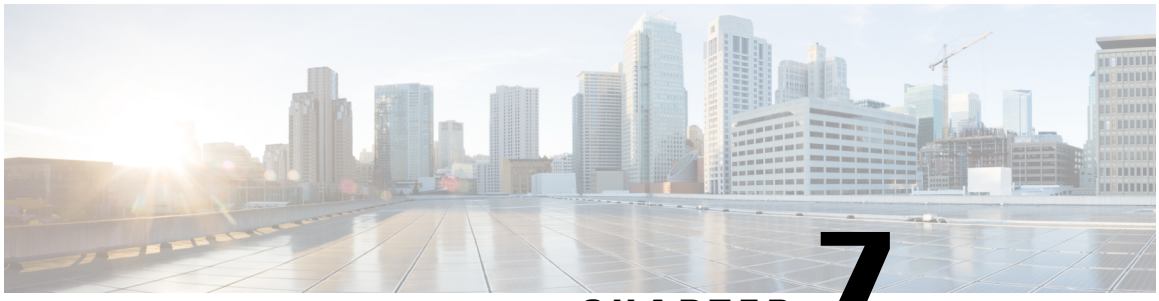
Feature Information for OSPFv3 External Path Preference Option

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: Feature Information for OSPFv3 External Path Preference Option

Feature Name	Releases	Feature Information
OSPFv3 External Path Preference Option	Cisco IOS XE Release 3.4S	This feature provides a way to calculate external path preferences per RFC 5340. The following commands were introduced or modified: **compatible rfc1583**, **show ospfv3**.



CHAPTER 7

OSPFv3 Graceful Restart

The graceful restart feature in Open Shortest Path First version 3 (OSPFv3) allows nonstop data forwarding along routes that are already known while the OSPFv3 routing protocol information is being restored.

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.

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 OSPFv3 Graceful Restart

OSPFv3 Graceful Restart

The graceful restart feature in OSPFv3 allows nonstop data forwarding along routes that are already known while the OSPFv3 routing protocol information is being restored. A device can participate in graceful restart either in restart mode (such as in a graceful-restart-capable device) or in helper mode (such as in a graceful-restart-aware device).

To perform the graceful restart function, a device must be in high availability (HA) stateful switchover (SSO) mode (that is, dual Route Processor (RP)). A device capable of graceful restart will perform the graceful restart function when the following failures occur:

- A RP failure that results in switchover to standby RP
- A planned RP switchover to standby RP

The graceful restart feature requires that neighboring devices be graceful-restart aware.

For further information about SSO and nonstop forwarding (NSF), see the Stateful Switchover and Cisco Nonstop Forwarding documents.

How to Enable OSPFv3 Graceful Restart

Enabling OSPFv3 Graceful Restart on a Graceful-Restart-Capable Router

The task can be performed in Cisco IOS XE 3.4S and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **graceful-restart** [**restart-interval** *interval*]

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 ospfv3** [*process-id*] **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

	Command or Action	Purpose
Step 4	**graceful-restart** [**restart-interval** *interval*] **Example:** `Router(config-rtr)# graceful-restart`	Enables the OSPFv3 graceful restart feature on a graceful-restart-capable router.

Enabling OSPFv3 Graceful Restart on a Graceful-Restart-Capable Router

The task can be performed in releases prior to Cisco IOS XE Release 3.4S.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart** [**restart-interval** *interval*]

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	**ipv6 router ospf** *process-id* **Example:** `Router(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**graceful-restart** [**restart-interval** *interval*] **Example:** `Router(config-rtr)# graceful-restart`	Enables the OSPFv3 graceful restart feature on a graceful-restart-capable router.

Enabling OSPFv3 Graceful Restart on a Graceful-Restart-Aware Router

The task can be performed in Cisco IOS XE Release 3.4S and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**

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 ospfv3** [*process-id*] **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**graceful-restart helper** {**disable**	**strict-lsa-checking** **Example:** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	Enables the OSPFv3 graceful restart feature on a graceful-restart-aware router.

Example:

What to Do Next

Enabling OSPFv3 Graceful Restart on a Graceful-Restart-Aware Router

The task can be performed in releases prior to Cisco IOS XE Release 3.4S.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **graceful-restart helper** {**disable** | **strict-lsa-checking**

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	**ipv6 router ospf** *process-id* **Example:** `Router(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**graceful-restart helper** {**disable**	**strict-lsa-checking** **Example:** `Router(config-rtr)# graceful-restart helper strict-lsa-checking`	Enables the OSPFv3 graceful restart feature on a graceful-restart-aware router.

Example:

What to Do Next

Configuration Examples for OSPFv3 Graceful Restart

Example: Enabling OSPFv3 Graceful Restart

```
Router# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
 Graceful Restart enabled
    restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
  Graceful Restart helper support enabled
  Router status : Active
  Router is running in SSO mode
  OSPF restart state : NO_RESTART
  Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

The following example shows OSPFv3 information with graceful-restart helper support enabled on a graceful-restart-aware router.

```
Router# show ospfv3
 Routing Process "ospfv3 1" with ID 10.0.0.1
 Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 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 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Stateful switchover and Cisco nonstop forwarding	*High Availability Configuration Guide*

Related Topic	Document Title
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
OSPFv3 Graceful Restart	"*OSPF RFC 3623 Graceful Restart Helper Mode*" module
OSPFv3 Graceful Restart	"*Configuring OSPF* " module
OSPFv3 Graceful Restart	"*NSF-OSPF RFC 3623 OSPF Graceful Restart* " 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

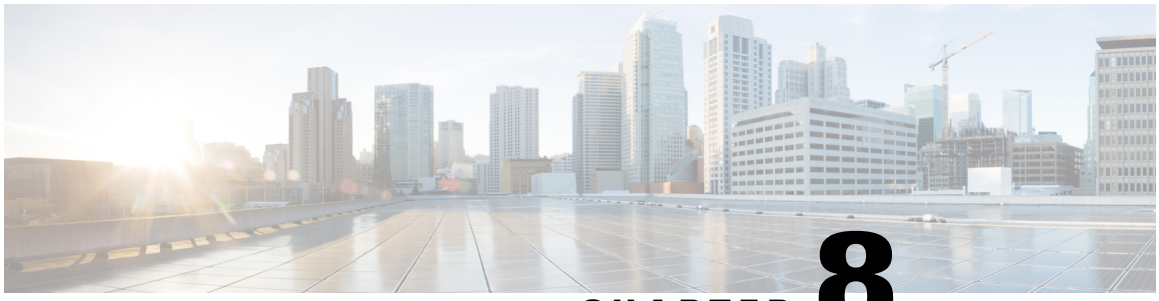
Feature Information for OSPFv3 Graceful Restart

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 10: Feature Information for OSPFv3 Graceful Restart

Feature Name	Releases	Feature Information
OSPFv3 Graceful Restart	Cisco IOS XE Release 2.1	The graceful restart feature in OSPFv3 allows nonstop data forwarding along routes that are already known while the OSPFv3 routing protocol information is being restored. The following commands were introduced or modified: **graceful-restart**, **graceful-restart helper**, **ipv6 router ospf**, **router ospfv3**, **show ipv6 ospf graceful-restart**, **show ospfv3 graceful-restart**.



CHAPTER 8

Graceful Shutdown Support for OSPFv3

This feature provides the ability to temporarily shut down an Open Shortest Path First version 3 (OSPFv3) process or interface 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 OSPFv3 interfaces or on a specific interface.

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.

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 Graceful Shutdown Support for OSPFv3

OSPFv3 Graceful Shutdown

The Graceful Shutdown for OSPFv3 feature provides the ability to temporarily shut down the OSPFv3 protocol in the least disruptive manner and to 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 OSPFv3 protocol can be initiated using the **shutdown** command in router configuration mode or in address family configuration mode.

This feature also provides the ability to shut down OSPFv3 on a specific interface. In this case, OSPFv3 will not advertise the interface or form adjacencies over it; however, all of the OSPFv3 interface configuration will be retained. To initiate a graceful shutdown of an interface, use the **ipv6 ospf shutdown** or the **ospfv3 shutdown** command in interface configuration mode.

How to Configure Graceful Shutdown Support for OSPFv3

Configuring Graceful Shutdown of the OSPFv3 Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ipv6 router ospf** *process-id*
   - **router ospfv3** *process-id*
4. **shutdown**
5. **end**
6. Do one of the following:
   - **show ipv6 ospf** [*process-id*]
   - **show ospfv3** [*process-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	Do one of the following: • **ipv6 router ospf** *process-id* • **router ospfv3** *process-id*	Enables OSPFv3 routing and enters router configuration mode.

	Command or Action	Purpose

	Example:
	`Device(config)# ipv6 router ospf 1`
	
	Example:
	`Device(config)# router ospfv3 101`	

Step 4	**shutdown** **Example:** `Device(config-router)# shutdown`	Shuts down the selected interface.
Step 5	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.

Step 6	Do one of the following:
	• **show ipv6 ospf** [*process-id*]
	• **show ospfv3** [*process-id*]
	
	Example:
	`Device# show ipv6 ospf`
	
	Example:
	`Device# show ospfv3`
		(Optional) Displays general information about OSPFv3 routing processes.

Configuring Graceful Shutdown of the OSPFv3 Process in Address-Family Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast** [**vrf** *vrf-name*]
5. **shutdown**
6. **end**
7. **show ospfv3** [*process-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`	Enables router configuration mode for the IPv6 address family.
Step 4	**address-family ipv6 unicast** [**vrf** *vrf-name*] **Example:** `Device(config-router)#address-family ipv6`	Enters IPv6 address family configuration mode for OSPFv3.
Step 5	**shutdown** **Example:** `Device(config-router-af)# shutdown`	Shuts down the selected interface.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Returns to privileged EXEC mode.
Step 7	**show ospfv3** [*process-id*] **Example:** `Device# show ospfv3`	(Optional) Displays general information about OSPFv3 routing processes.

Configuring OSPFv3 Graceful Shutdown of the OSPFv3 Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ipv6 ospf shutdown**
   - **ospfv3 shutdown**
5. **end**
6. **show ospfv3** *process-id* [*area-id*] [*address-family*] [**vrf** {*vrf-name* | ***** }] **interface** [*type number*] [**brief**]

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 GigabitEthernet`	Configures an interface type and number and enters interface configuration mode.
Step 4	Do one of the following: • **ipv6 ospf shutdown** • **ospfv3 shutdown** **Example:** `Device(config-if)# ipv6 ospf shutdown`	Initiates an OSPFv3 protocol graceful shutdown at the interface level. • When the **ipv6 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 OSPFv3 traffic around this device.

	Command or Action	Purpose
	Example: `Device(config-if)# ospfv3 process-id ipv6 shutdown`	
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ospfv3** *process-id* [*area-id*] [*address-family*] [**vrf** {*vrf-name* | ***** }] **interface** [*type number*] [**brief**] **Example:** `Device# show ospfv3 1 interface`	(Optional) Displays OSPFv3-related interface information.

Configuration Examples for Graceful Shutdown Support for OSPFv3

Example: Configuring Graceful Shutdown of the OSPFv3 Process

The following example shows how to configure graceful shutdown of the OSPFv3 process in IPv6 router OSPF configuration mode configuration mode:

```
ipv6 router ospf 6
 router-id 10.10.10.10
 shutdown
```

The following example shows how to configure graceful shutdown of the OSPFv3 process in router OSPFv3 configuration mode:

```
!
router ospfv3 1
 shutdown
 !
 address-family ipv6 unicast
  exit-address-family
```

The following example shows how to configure graceful shutdown of the OSPFv3 process in address-family configuration mode:

```
!
router ospfv3 1
 !
 address-family ipv6 unicast
  shutdown
  exit-address-family
```

Example: Configuring Graceful Shutdown of the OSPFv3 Interface

The following example shows how to configure graceful shutdown of the OSPFv3 interface using the **ipv6 ospf shutdown** command:

```
!
interface Serial2/1
 no ip address
 ipv6 enable
 ipv6 ospf 6 area 0
 ipv6 ospf shutdown
 serial restart-delay 0
 end
```

The following example shows how to configure graceful shutdown of the OSPFv3 interface using the **ospfv3 shutdown** command:

```
!
interface Serial2/0
 ip address 10.10.10.10 255.255.255.0
 ip ospf 1 area 0
 ipv6 enable
 ospfv3 shutdown
 ospfv3 1 ipv6 area 0
 serial restart-delay 0
 end
```

Additional References for Graceful Shutdown Support for OSPFv3

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Cisco IOS commands	Cisco IOS Master Command List, All Releases

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

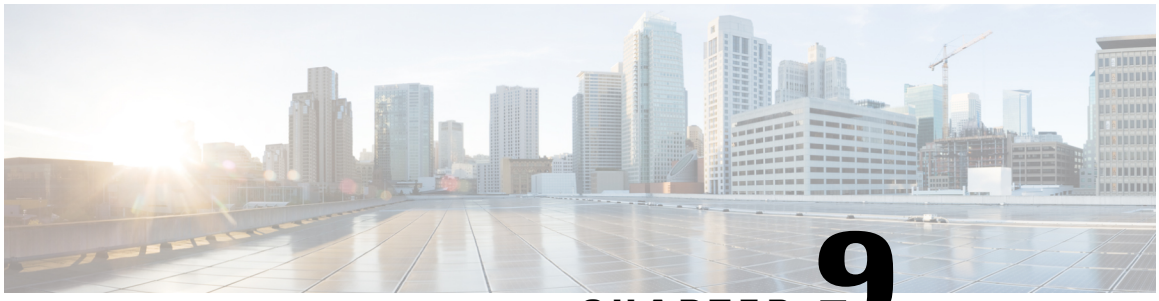
Feature Information for Graceful Shutdown Support for OSPFv3

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 11: Feature Information for Graceful Shutdown Support for OSPFv3

Feature Name	Releases	Feature Information
Graceful Shutdown Support for OSPFv3	Cisco IOS XE Release 3.8	This feature provides the ability to temporarily shut down an Open Shortest Path First version 3 (OSPFv3) process or interface 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 OSPFv3 interfaces or on a specific interface. The following commands were introduced: • **ipv6 ospf shutdown** • **ospfv3 shutdown** • **shutdown (router ospfv3)**



CHAPTER 9

OSPF Stub Router Advertisement

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks.

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.

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 Stub Router Advertisement

OSPF Stub Router Advertisement Functionality

The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. This feature introduces three configuration

options that allow you to configure a router that is running the Open Shortest Path First (OSPF) protocol to advertise a maximum or infinite metric to all neighbors.

When any of these three configuration options are enabled on a router, the router will originate link-state advertisements (LSAs) with a maximum metric (LSInfinity: 0xFFFF) through all nonstub links. The advertisement of a maximum metric causes other routers to assign a cost to the new router that is higher than the cost of using an alternate path. Because of the high cost assigned to paths that pass through the new router, other routers will not use a path through the new router as a transit path to forward traffic that is destined for other networks, which allows switching and routing functions to be up and running and routing tables to converge before transit traffic is routed through this router.

Note Directly connected links in a stub network are not affected by the configuration of a maximum or infinite metric because the cost of a stub link is always set to the output interface cost.

Maximum Metric Allows Routing Tables to Converge

Two configuration options introduced by the OSPF Stub Router Advertisement feature allow you to bring a new router into a network without immediately routing traffic through the new router. These configuration options are useful because Interior Gateway Protocols (IGPs) converge very quickly upon a router during startup or after a reload, often before Border Gateway Protocol (BGP) routing tables have completely converged. If neighbor routers forward traffic through a router while that router is building BGP routing tables, packets that have been received for other destinations may be dropped. Advertising a maximum metric during startup will allow routing tables to converge before traffic that is destined for other networks is sent through the router.

The following two configuration options enable a router to advertise a maximum metric at startup:

- You can configure a timer to advertise a maximum metric when the router is started or reloaded. When this option is configured, the router will advertise a maximum metric, which forces neighbor routers to select alternate paths until the timer expires. When the timer expires, the router will advertise accurate (normal) metrics, and other routers will send traffic to this router depending on the cost. The configurable range of the timer is from 5 to 86,400 seconds.
- You can configure a router to advertise a maximum metric at startup until BGP routing tables converge or until the default timer expires (600 seconds). Once BGP routing tables converge or the default timer expires, the router will advertise accurate (normal) metrics and other routers will send traffic to this router, depending on the cost.

Maximum Metric Allows Graceful Shutdown of a Router

The third configuration option introduced by the OSPF Stub Router Advertisement feature allows you to gracefully remove a router from the network by advertising a maximum metric through all links, which allows other routers to select alternate paths for transit traffic to follow before the router is shut down. There are many situations where you may need to remove a router from the network. If a router is removed from a network and neighbor routers cannot detect that the physical interface is down, neighbors will need to wait for dead timers to expire before the neighbors will remove the adjacency and routing tables will reconverge. This situation may occur when there is a switch between other routers and the router that is shut down. Packets may be dropped while the neighbor routing tables reconverge.

When this third option is configured, the router advertises a maximum metric, which allows neighbor routers to select alternate paths before the router is shut down. This configuration option could also be used to remove a router that is in a critical condition from the network without affecting traffic that is destined for other networks.

Note You should not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

Benefits of OSPF Stub Router Advertisement

Improved Stability and Availability

Advertising a maximum metric through all links at startup or during a reload will prevent neighbor routers from using a path through the router as a transit path, thereby reducing the number of packets that are dropped and improving the stability and availability of the network.

Graceful Removal from the Network

Advertising a maximum metric before shutdown allows other routers to select alternate paths before the transit path through a router becomes inaccessible.

How to Configure OSPF Stub Router Advertisement

The following tasks configure OSPF to advertise a maximum metric. This feature has three different configuration options. All tasks are optional and should be individually configured.

Configuring Advertisement on Startup

SUMMARY STEPS

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **max-metric router-lsa on-startup** *announce-time*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** *process-id*	Places the router in router configuration mode and enables an OSPF routing process.
Step 2	Router(config-router)# **max-metric router-lsa on-startup** *announce-time*	Configures OSPF to advertise a maximum metric during startup for a configured period of time. The *announce-time* argument is a configurable timer that must follow the **on-startup** keyword to be configured. There is

	Command or Action	Purpose
		no default timer value. The configurable time range is from 5 to 86,400 seconds.

Configuring Advertisement Until Routing Tables Converge

SUMMARY STEPS

1. Router(config)# **router ospf** *process-id*
2. Router(config-router)# **max-metric router-lsa on-startup wait-for-bgp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** *process-id*	Places the router in router configuration mode and enables an OSPF routing process.
Step 2	Router(config-router)# **max-metric router-lsa on-startup wait-for-bgp**	Configures OSPF to advertise a maximum metric until BGP routing tables have converged or until the default timer has expired. The **wait-for-bgp** keyword must follow the **on-startup** keyword to be configured. The default timer value is 600 seconds.

Configuring Advertisement for a Graceful Shutdown

SUMMARY STEPS

1. Router(config)# **router ospf**process-id
2. Router(config-router)# **max-metric router-lsa**
3. Router(config-router)# **end**
4. Router# **show ip ospf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf**process-id	Places the router in router configuration mode and enables an OSPF routing process.

	Command or Action	Purpose
Step 2	Router(config-router)# **max-metric router-lsa**	Configures OSPF to advertise a maximum metric until the router is shut down.
Step 3	Router(config-router)# **end**	Ends configuration mode and places the router in privileged EXEC mode.
Step 4	Router# **show ip ospf**	Displays general information about OSPF routing processes. • Use the **show ip ospf** command to verify that the **max-metric router-lsa** command has been enabled before the router is shut down or reloaded.

What to Do Next

Note Do not save the running configuration of a router when it is configured for a graceful shutdown because the router will continue to advertise a maximum metric after it is reloaded.

Verifying the Advertisement of a Maximum Metric

To verify that the advertisement of a maximum metric has been configured correctly, use the **show ip ospf**or **show ip ospf database**command.

The output of the **show ip ospf**command will display the condition, state, and remaining time delay of the advertisement of a maximum metric, depending on which options were configured with the **max-metric router-lsa** command.

The following sample output is similar to the output that will be displayed when the **on-startup**keyword and *announce-time* argument are configured with the **max-metric router-lsa** command:

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric, Time remaining: 00:01:18
        Condition: on startup for 300 seconds, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
     Number of opaque AS LSA 0. Checksum Sum 0x0
     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 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
```

```
          Number of LSA 8. Checksum Sum 0x474AE
          Number of opaque link LSA 0. Checksum Sum 0x0
```

The following sample output is similar to the output that will be displayed when the **on-startup**and **wait-for-bgp** keywords are configured with the **max-metric router-lsa** command:

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric, Time remaining: 00:01:18
        Condition: on startup while BGP is converging, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
     Number of opaque AS LSA 0. Checksum Sum 0x0
     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 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
           Number of LSA 8. Checksum Sum 0x474AE
           Number of opaque link LSA 0. Checksum Sum 0x0
```

The following sample output is similar to the output that will be displayed when the **max-metric router-lsa** command is configured without any keywords or arguments:

```
Router# show ip ospf
Routing Process "ospf 1998" with ID 10.18.134.155
     Supports only single TOS(TOS0) routes
     Supports opaque LSA
     It is an area border and autonomous system boundary router
     Redistributing External Routes from,
        static, includes subnets in redistribution
     Originating router-LSAs with maximum metric
        Condition: always, State: active
     SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
     Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
     Number of external LSA 7. Checksum Sum 0x47261
     Number of opaque AS LSA 0. Checksum Sum 0x0
     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 2. 1 normal 0 stub 1 nssa
     External flood list length 0
        Area BACKBONE(0)
           Number of interfaces in this area is 1
           Area has no authentication
           SPF algorithm executed 3 times
           Area ranges are
           Number of LSA 8. Checksum Sum 0x474AE
           Number of opaque link LSA 0. Checksum Sum 0x0
```

The output of the **show ip ospf database**command will display information about OSPF LSAs and indicate if the router is announcing maximum cost links. The following sample output is similar to the output that will be displayed when any form of the **max-metric router-lsa** command is configured:

```
Router# show ip ospf database
      Exception Flag: Announcing maximum link costs
      LS age: 68
      Options: (No TOS-capability, DC)
      LS Type: Router Links
      Link State ID: 172.18.134.155
      Advertising Router: 172.18.134.155
      LS Seq Number: 80000002
```

```
Checksum: 0x175D
Length: 60
Area Border Router
AS Boundary Router
Number of Links: 3

  Link connected to: a Transit Network
  (Link ID) Designated Router address: 192.168.1.11
  (Link Data) Router Interface address: 192.168.1.14
   Number of TOS metrics: 0
    TOS 0 Metrics: 65535 (metric used for local calculation: 10)

  Link connected to: a Transit Network
  (Link ID) Designated Router address: 10.1.145.11
  (Link Data) Router Interface address: 10.1.145.14
   Number of TOS metrics: 0
    TOS 0 Metrics: 65535 (metric used for local calculation: 10)

  Link connected to: a Stub Network
  (Link ID) Network/subnet number: 10.11.12.0
  (Link Data) Network Mask: 255.255.255.0
   Number of TOS metrics: 0
    TOS 0 Metrics: 1
```

Monitoring and Maintaining OSPF Stub Router Advertisement

Command	Purpose
`Router#` **show ip ospf**	Displays general information about OSPF routing processes and provides information about the configuration settings and status of the OSPF Stub Router Advertisement feature.
`Router#` **show ip ospf database router**	Displays information about router LSAs, and indicates if a router is announcing maximum link costs.

Configuration Examples of OSPF Stub Router Advertisement

Example Advertisement on Startup

In the following example, a router that is running OSPF is configured to advertise a maximum metric at startup for 300 seconds:

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa on-startup 300
```

Example Advertisement Until Routing Tables Converge

In the following example, a router that is running OSPF is configured to advertise a maximum metric until BGP routing tables converge or until the default timer expires (600 seconds):

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa on-startup wait-for-bgp
```

Example Graceful Shutdown

In the following example, a router that is running OSPF is configured to advertise a maximum metric until the router is shut down:

```
Router(config)# router ospf 100
 Router(config-router)# max-metric router-lsa
 Router(config-router)# end
 Router# show ip ospf
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF" in the *IP Routing: OSPF Configuration Guide*.
OSPFv2 loop-free alternate fast reroute	"OSPFv2 Loop-Free Alternate Fast Reroute" in the *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard/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

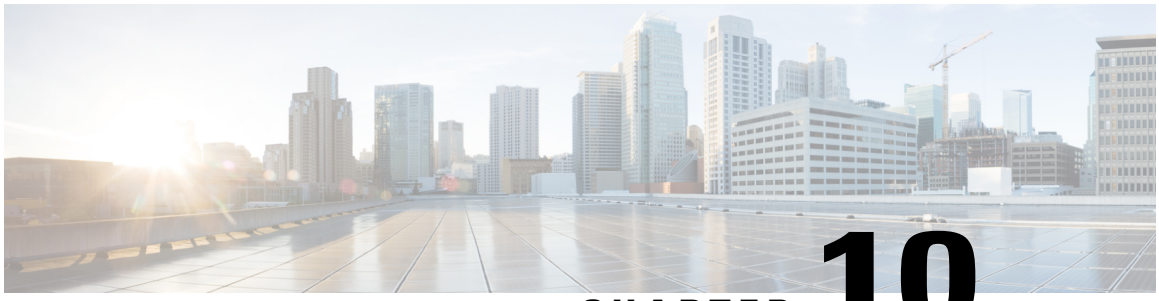
Feature Information for OSPF Stub Router Advertisement

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 12: Feature Information for OSPF Stub Router Advertisement

Feature Name	Releases	Feature Information
OSPF Stub Router Advertisement	Cisco IOS XE Release 2.1	The OSPF Stub Router Advertisement feature allows you to bring a new router into a network without immediately routing traffic through the new router and allows you to gracefully shut down or reload a router without dropping packets that are destined for other networks. The following commands are introduced or modified in the feature documented in this module: • **max-metric router-lsa** • **show ip ospf**



CHAPTER 10

OSPF Update Packet-Pacing Configurable Timers

This module describes the OSPF Update Packet-Pacing Configurable Timers feature, which allows you to configure the rate at which OSPF LSA flood pacing, retransmission pacing, and group pacing updates occur.

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.

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 on OSPF Update Packet-Pacing Configurable Timers

Do not change the packet-pacing timers unless all other options to meet OSPF packet flooding requirements have been exhausted. Specifically, network operators should prefer summarization, stub area usage, queue tuning, and buffer tuning before changing the default timers. Furthermore, there are no guidelines for changing timer values; each OSPF deployment is unique and should be considered on a case-by-case basis. The network operator assumes risks that are associated with changing the default timer values.

Information About OSPF Update Packet-Pacing Configurable Timers

Functionality of the OSPF Update Packet-Pacing Timers

In rare situations, you might need to change Open Shortest Path First (OSPF) packet-pacing default timers to mitigate CPU or buffer utilization issues associated with flooding very large numbers of link-state advertisements (LSAs). The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which OSPF LSA flood pacing, retransmission pacing, and group pacing updates occur.

- Configuring OSPF flood pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF transmission queue.
- Configuring OSPF retransmission pacing timers allows you to control interpacket spacing between consecutive link-state update packets in the OSPF retransmission queue.
- Cisco IOS XE software groups the periodic refresh of LSAs to improve the LSA packing density for the refreshes in large topologies. The group timer controls the interval that is used for group LSA refreshment; however, this timer does not change the frequency at which individual LSAs are refreshed (the default refresh occurs every 30 minutes).

Caution The default settings for OSPF packet-pacing timers are suitable for the majority of OSPF deployments. You should change the default timers only as a last resort.

Benefits of OSPF Update Packet-Pacing Configurable Timers

The OSPF Update Packet-Pacing Configurable Timers feature provides the administrator with a mechanism to control the rate at which LSA updates occur in order to reduce high CPU or buffer utilization that can occur when an area is flooded with a very large number of LSAs.

How to Configure OSPF Packet-Pacing Timers

The tasks in this section describe how to configure and verify three OSPF update packet-pacing timers.

Configuring OSPF Packet-Pacing Timers

Caution The default settings for OSPF packet-pacing timers are suitable for the majority of OSPF deployments. You should change the default timers only as a last resort.

To configure a flood packet-pacing timer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing flood** milliseconds

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** process-id	Places the router in router configuration mode and enables an OSPF routing process.
Step 2	Router(config-router)# **timers pacing flood** milliseconds	Configures a flood packet-pacing timer delay (in milliseconds).

Configuring a Retransmission Packet-Pacing Timer

To configure a retransmission packet-pacing timer, use the following commands beginning in global configuration mode:

SUMMARY STEPS

1. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing retransmission** milliseconds

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** process-id	Places the router in router configuration mode and enables an OSPF routing process.
Step 2	Router(config-router)# **timers pacing retransmission** milliseconds	Configures a retransmission packet-pacing timer delay (in milliseconds).

Configuring a Group Packet-Pacing Timer

To configure a group packet-pacing timer, use the following commands beginning in router configuration mode:

SUMMARY STEPS

1. Router(config)# **router ospf** process-id
2. Router(config-router)# **timers pacing lsa-group** seconds

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# **router ospf** process-id	Places the router in router configuration mode and enables an OSPF routing process.
Step 2	Router(config-router)# **timers pacing lsa-group** seconds	Configures an LSA group packet-pacing timer delay (in seconds).

Verifying OSPF Packet-Pacing Timers

To verify that OSPF packet pacing has been configured, use the show ip ospf privileged EXEC command. The output of the show ip ospf command will display the type and delay time of the configurable pacing timers (flood, retransmission, group). The following sample output is from the show ip ospf command:

```
Router# show ip ospf
  Routing Process "ospf 1" with ID 10.0.0.1 and Domain ID 10.20.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  LSA group pacing timer 100 secs
  Interface flood pacing timer 55 msecs
  Retransmission pacing timer 100 msecs
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  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 2. 2 normal 0 stub 0 nssa
  External flood list length 0
     Area BACKBONE(0)
         Number of interfaces in this area is 2
         Area has message digest authentication
         SPF algorithm executed 4 times
         Area ranges are
         Number of LSA 4. Checksum Sum 0x29BEB
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 3
         Number of indication LSA 0
         Number of DoNotAge LSA 0
         Flood list length 0
     Area 172.16.26.0
         Number of interfaces in this area is 0
         Area has no authentication
         SPF algorithm executed 1 times
         Area ranges are
            192.168.0.0/16 Passive Advertise
         Number of LSA 1. Checksum Sum 0x44FD
         Number of opaque link LSA 0. Checksum Sum 0x0
         Number of DCbitless LSA 1
         Number of indication LSA 1
```

```
Number of DoNotAge LSA 0
Flood list length 0
```

Troubleshooting Tips

If the number of OSPF packet retransmissions rapidly increases, increase the value of the packet-pacing timers. The number of OSPF packet retransmissions is displayed in the output of the show ip ospf neighbor command.

Monitoring and Maintaining OSPF Packet-Pacing Timers

Command	Purpose
`Router#` **show ip ospf**	Displays general information about OSPF routing processes.
`router#` **show ip ospf neighbor**	Displays OSPF neighbor information on a per-interface basis.
`Router#` **clear ip ospf redistribution**	Clears route redistribution based on the OSPF routing process ID.

Configuration Examples of OSPF Update Packet-Pacing

Example LSA Flood Pacing

The following example configures LSA flood pacing updates to occur in 50-millisecond intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing flood 50
```

Example LSA Retransmission Pacing

The following example configures LSA retransmission pacing updates to occur in 100-millisecond intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing retransmission 100
```

Example LSA Group Pacing

The following example configures OSPF group pacing updates between LSA groups to occur in 75-second intervals for OSPF routing process 1:

```
Router(config)# router ospf 1
Router(config-router)# timers pacing lsa-group 75
```

Additional References

For additional information related to the OSPF Update Packet-Pacing Configurable Timers feature, see the following references:

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 software releases , and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

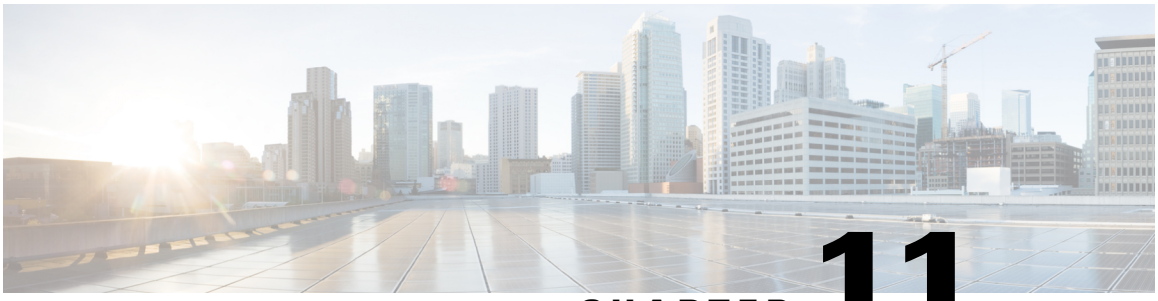
Feature Information for OSPF Update Packet-Pacing Configurable Timers

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 13: Feature Information for OSPF Update Packet-Pacing Configurable Timers

Feature Name	Releases	Feature Information
OSPF Update Packet-Pacing Configurable Timers	Cisco IOS XE Release 2.1	The OSPF Update Packet-Pacing Configurable Timers feature allows you to configure the rate at which OSPF LSA flood pacing, retransmission pacing, and group pacing updates occur. The following commands are introduced or modified in the feature documented in this module: • **timers pacing flood** • **timers pacing lsa-group** • **timers pacing retransmission** • **show ip ospf**



CHAPTER 11

OSPF Sham-Link Support for MPLS VPN

This document describes how to configure and use a sham-link to connect Virtual Private Network (VPN) client sites that run the Open Shortest Path First (OSPF) protocol and share backdoor OSPF links in a Multiprotocol Label Switching (MPLS) VPN 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.

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

Prerequisites for OSPF Sham-Link Support for MPLS VPN

Before you can configure a sham-link in an MPLS VPN, you must first enable OSPF as follows:

- Create an OSPF routing process.

- Specify the range of IP addresses to be associated with the routing process.
- Assign area IDs to be associated with the range of IP addresses.

Restrictions on OSPF Sham-Link Support for MPLS VPN

When OSPF is used as a protocol between PE and CE routers, the OSPF metric is preserved when routes are advertised over the VPN backbone. The metric is used on the remote PE routers to select the correct route. For this reason, you should not modify the metric value when OSPF is redistributed to BGP, and when BGP is redistributed to OSPF. If you modify the metric value, routing loops may occur.

Information About OSPF Sham-Link Support for MPLS VPN

Benefits of OSPF Sham-Link Support for MPLS VPN

Client Site Connection Across the MPLS VPN Backbone

A sham-link overcomes the OSPF default behavior for selecting an intra-area backdoor route between VPN sites instead of an interarea (PE-to-PE) route. A sham-link ensures that OSPF client sites that share a backdoor link can communicate over the MPLS VPN backbone and participate in VPN services.

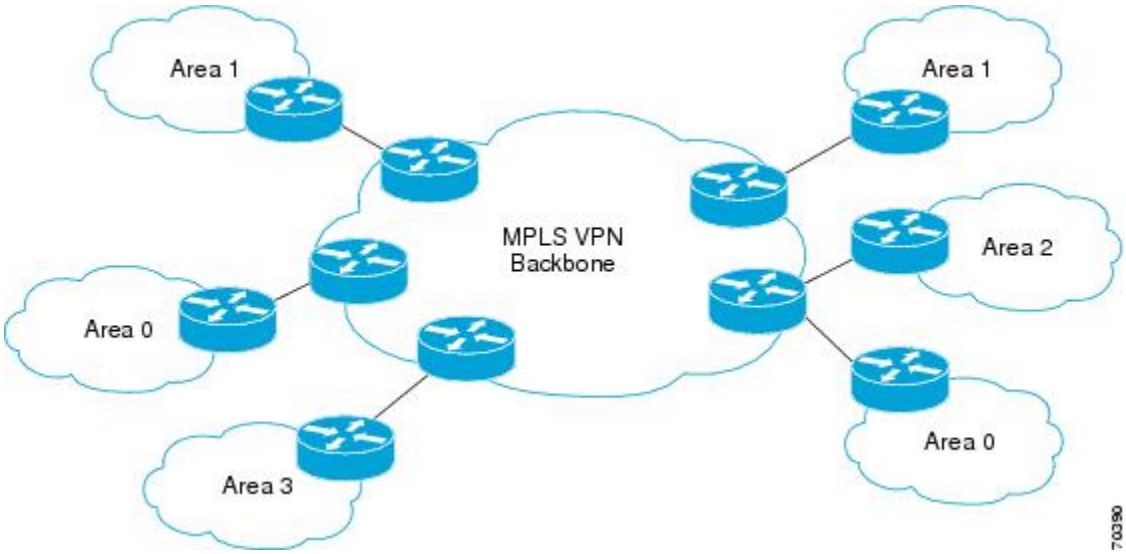
Flexible Routing in an MPLS VPN Configuration

In an MPLS VPN configuration, the OSPF cost configured with a sham-link allows you to decide if OSPF client site traffic will be routed over a backdoor link or through the VPN backbone.

Using OSPF in PE-CE Router Connections

In an MPLS VPN configuration, the OSPF protocol is one way you can connect customer edge (CE) routers to service provider edge (PE) routers in the VPN backbone. OSPF is often used by customers who run OSPF as their intrasite routing protocol, subscribe to a VPN service, and want to exchange routing information between their sites using OSPF (during migration or on a permanent basis) over an MPLS VPN backbone.

The figure below shows an example of how VPN client sites that run OSPF can connect over an MPLS VPN backbone.



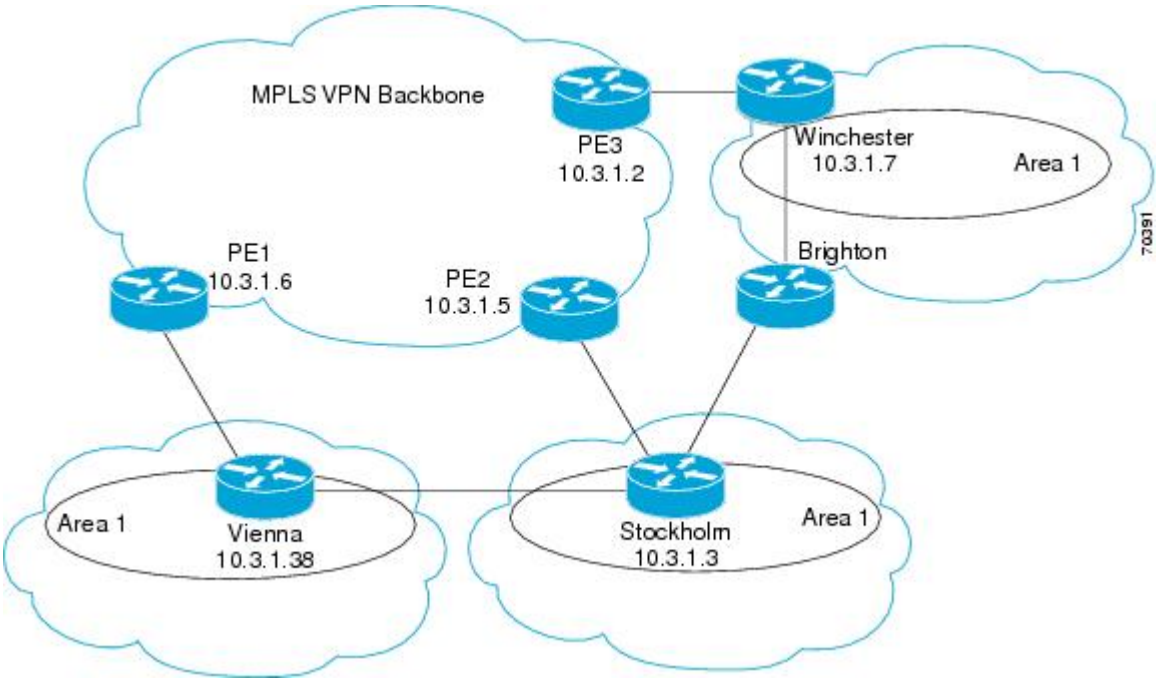
When OSPF is used to connect PE and CE routers, all routing information learned from a VPN site is placed in the VPN routing and forwarding (VRF) instance associated with the incoming interface. The PE routers that attach to the VPN use the Border Gateway Protocol (BGP) to distribute VPN routes to each other. A CE router can then learn the routes to other sites in the VPN by peering with its attached PE router. The MPLS VPN superbackbone provides an additional level of routing hierarchy to interconnect the VPN sites running OSPF.

When OSPF routes are propagated over the MPLS VPN backbone, additional information about the prefix in the form of BGP extended communities (route type, domain ID extended communities) is appended to the BGP update. This community information is used by the receiving PE router to decide the type of link-state advertisement (LSA) to be generated when the BGP route is redistributed to the OSPF PE-CE process. In this way, internal OSPF routes that belong to the same VPN and are advertised over the VPN backbone are seen as interarea routes on the remote sites.

For basic information about how to configure an MPLS VPN, refer to the *Cisco IOS XE MPLS Configuration Guide, Release 2*.

Using a Sham-Link to Correct OSPF Backdoor Routing

Although OSPF PE-CE connections assume that the only path between two client sites is across the MPLS VPN backbone, backdoor paths between VPN sites (shown in grey in the figure below) may exist. If these sites belong to the same OSPF area, the path over a backdoor link will always be selected because OSPF prefers intraarea paths to interarea paths. (PE routers advertise OSPF routes learned over the VPN backbone as interarea paths.) For this reason, OSPF backdoor links between VPN sites must be taken into account so that routing is performed based on policy.



For example, the figure above shows three client sites, each with backdoor links. Because each site runs OSPF within the same Area 1 configuration, all routing between the three sites follows the intraarea path across the backdoor links, rather than over the MPLS VPN backbone.

The following example shows BGP routing table entries for the prefix 10.3.1.7/32 in the PE-1 router in the figure above. This prefix is the loopback interface of the Winchester CE router. As shown in bold in this example, the loopback interface is learned via BGP from PE-2 and PE-3. It is also generated through redistribution into BGP on PE-1.

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 58
Paths: (3 available, best #2)
  Advertised to non peer-group peers:
  10.3.1.2 10.3.1.5
  Local
    10.3.1.5 (metric 30) from 10.3.1.5 (10.3.1.5)
      Origin incomplete, metric 22, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.2.1.38 from 0.0.0.0 (10.3.1.6)
      Origin incomplete, metric 86, localpref 100, weight 32768,
      valid, sourced, best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

Within BGP, the locally generated route (10.2.1.38) is considered to be the best route. However, as shown in bold in the next example, the VRF routing table shows that the selected path is learned via OSPF with a next hop of 10.2.1.38, which is the Vienna CE router.

```
PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
```

```
  Known via "ospf 100", distance 110, metric 86, type intra area
  Redistributing via bgp 215
  Advertised by bgp 215
  Last update from 10.2.1.38 on Serial0/0/0, 00:00:17 ago
  Routing Descriptor Blocks:
  * 10.2.1.38
, from 10.3.1.7, 00:00:17 ago, via Serial0/0/0
      Route metric is 86, traffic share count is 1
```

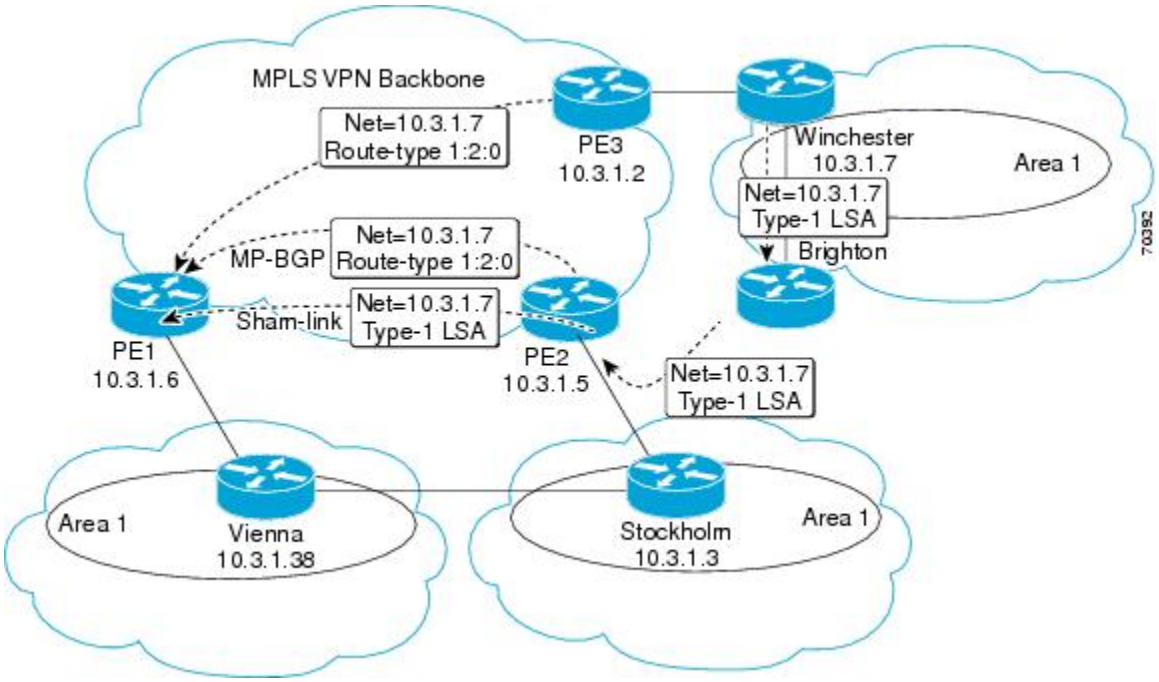
This path is selected because:

- The OSPF intra-area path is preferred over the interarea path (over the MPLS VPN backbone) generated by the PE-1 router.
- OSPF has a lower administrative distance (AD) than internal BGP (BGP running between routers in the same autonomous system).

If the backdoor links between sites are used only for backup purposes and do not participate in the VPN service, then the default route selection shown in the preceding example is not acceptable. To reestablish the desired path selection over the MPLS VPN backbone, you must create an additional OSPF intra-area (logical) link between ingress and egress VRFs on the relevant PE routers. This link is called a sham-link.

A sham-link is required between any two VPN sites that belong to the same OSPF area and share an OSPF backdoor link. If no backdoor link exists between the sites, no sham-link is required.

The figure below shows a sample sham-link between PE-1 and PE-2. A cost is configured with each sham-link and is used to decide whether traffic will be sent over the backdoor path or the sham-link path. When a sham-link is configured between PE routers, the PEs can populate the VRF routing table with the OSPF routes learned over the sham-link.



Because the sham-link is seen as an intra-area link between PE routers, an OSPF adjacency is created and database exchange (for the particular OSPF process) occurs across the link. The PE router can then flood LSAs between sites from across the MPLS VPN backbone. As a result, the desired intra-area connectivity is created.

How to Configure an OSPF Sham-Link

Creating a Sham-Link

Before You Begin

Before you create a sham-link between PE routers in an MPLS VPN, you must:

- Configure a separate /32 address on the remote PE so that OSPF packets can be sent over the VPN backbone to the remote end of the sham-link. The /32 address must meet the following criteria:
  - Belong to a VRF.
  - Not be advertised by OSPF.
  - Be advertised by BGP.

You can use the /32 address for other sham-links.

- Associate the sham-link with an existing OSPF area.

To create a sham-link, use the following commands starting in EXEC mode:

SUMMARY STEPS

1. Router1# **configure terminal**
2. Router1(config)# **ip vrf** *vrf-name*
3. Router1(config-vrf)# **exit**
4. Router1(config)# **interface loopback** *interface-number*
5. Router1(config-if)# **ip vrf forwarding** *vrf-name*
6. Router1(config-if)# **ip address** *ip-address mask*
7. Router1(config-if)# **end**
8. Router1(config)# **end**
9. Router2# **configure terminal**
10. Router2(config)# **interface loopback** *interface-number*
11. Router2(config-if)# **ip vrf forwarding** *vrf-name*
12. Router2(config-if)# **ip address** *ip-address mask*
13. Router2(config-if)# **end**
14. Router1(config)# **end**
15. Router1(config)# **router ospf** *process-id* **vrf** *vrf-name*
16. Router1(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*
17. Router2(config)# **router ospf** *process-id* **vrf** *vrf-name*
18. Router2(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router1# **configure terminal**	Enters global configuration mode on the first PE router.
Step 2	Router1(config)# **ip vrf** *vrf-name*	Defines a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 3	Router1(config-vrf)# **exit**	Exits VRF configuration mode and returns to global confiuration mode.
Step 4	Router1(config)# **interface loopback** *interface-number*	Creates a loopback interface to be used as an endpoint of the sham-link on PE-1 and enters interface configuration mode.
Step 5	Router1(config-if)# **ip vrf forwarding** *vrf-name*	Associates the loopback interface with a VRF. Removes the IP address.
Step 6	Router1(config-if)# **ip address** *ip-address mask*	Reconfigures the IP address of the loopback interface on PE-1.
Step 7	Router1(config-if)# **end**	Returns to global configuration mode.
Step 8	Router1(config)# **end**	Returns to EXEC mode.
Step 9	Router2# **configure terminal**	Enters global configuration mode on the second PE router.
Step 10	Router2(config)# **interface loopback** *interface-number*	Creates a loopback interface to be used as the endpoint of the sham-link on PE-2 and enters interface configuration mode.
Step 11	Router2(config-if)# **ip vrf forwarding** *vrf-name*	Associates the second loopback interface with a VRF. Removes the IP address.
Step 12	Router2(config-if)# **ip address** *ip-address mask*	Reconfigures the IP address of the loopback interface on PE-2.
Step 13	Router2(config-if)# **end**	Returns to global configuration mode.
Step 14	Router1(config)# **end**	Returns to EXEC mode.
Step 15	Router1(config)# **router ospf** *process-id* **vrf** *vrf-name*	Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-1 and enters interface configuration mode.
Step 16	Router1(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	Configures the sham-link on the PE-1 interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. **cost** *number* configures the OSPF cost for sending an IP packet on the PE-1 sham-link interface.
Step 17	Router2(config)# **router ospf** *process-id* **vrf** *vrf-name*	Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-2 and enters interface configuration mode.
Step 18	Router2(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	Configures the sham-link on the PE-2 interface within a specified OSPF area and with the loopback interfaces specified by the IP

	Command or Action	Purpose
		addresses as endpoints. **cost** *number* configures the OSPF cost for sending an IP packet on the PE-2 sham-link interface.

Verifying Sham-Link Creation

To verify that the sham-link was successfully created and is operational, use the **show ip ospf sham-links** command in EXEC mode:

```
Router# show ip ospf sham-links
Sham Link OSPF_SL0 to address 10.2.1.2 is up
Area 1 source address 10.2.1.1
  Run as demand circuit
  DoNotAge LSA allowed. Cost of using 40 State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Hello due in 00:00:04
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 4, number of
    retransmission 0
    First 0x63311F3C(205)/0x63311FE4(59) Next
    0x63311F3C(205)/0x63311FE4(59)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
    Link State retransmission due in 360 msec
```

Monitoring and Maintaining a Sham-Link

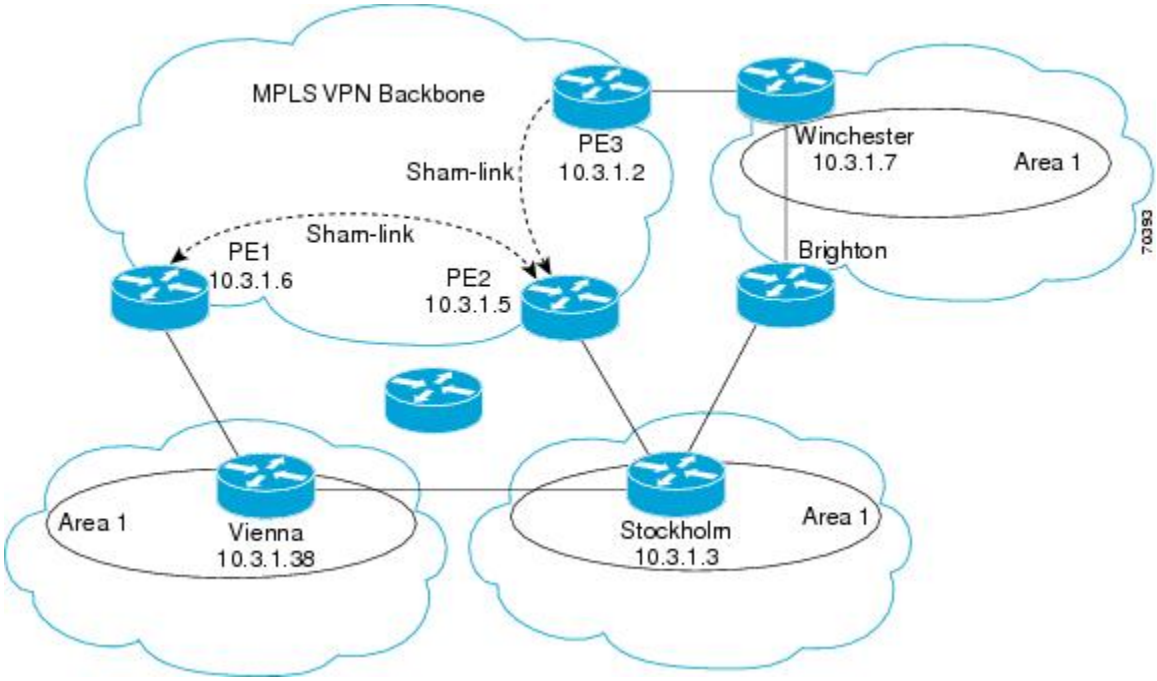
Command	Purpose
`Router#` **show ip ospf sham-links**	Displays the operational status of all sham-links configured for a router.
`Router#` **show ip ospf data router** *ip-address*	Displays information about how the sham-link is advertised as an unnumbered point-to-point connection between two PE routers.

Configuration Examples of an OSPF Sham-Link

Example Sham-Link Configuration

This example is designed to show how a sham-link is used only to affect the OSPF intra-area path selection of the PE and CE routers. The PE router also uses the information received from MP-BGP to set the outgoing label stack of incoming packets, and to decide to which egress PE router to label switch the packets.

The figure below shows a sample MPLS VPN topology in which a sham-link configuration is necessary. A VPN client has three sites, each with a backdoor link. Two sham-links have been configured, one between PE-1 and PE-2, and another between PE-2 and PE-3. A sham-link between PE-1 and PE-3 is not necessary in this configuration because the Vienna and Winchester sites do not share a backdoor link.



The following output shows the forwarding that occurs between sites from the standpoint of how PE-1 views the 10.3.1.7/32 prefix, the loopback1 interface of the Winchester CE router in the figure.

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 124
Paths: (1 available, best #1)
  Local
    10.3.1.2 (metric 30) from 10.3.1.2
 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100
", distance 110, metric 13, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:12:59 ago
  Routing Descriptor Blocks:
10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:12:59 ago
```

The following output shows forwarding information in which the next hop for the route, 10.3.1.2, is the PE-3 router rather than the PE-2 router (which is the best path according to OSPF). The reason the OSPF route is not redistributed to BGP on the PE is because the other end of the sham-link already redistributed the route to BGP and there is no need for duplication. The OSPF sham-link is used only to influence intra-area path selection. When sending traffic to a particular destination, the PE router uses the MP-BGP forwarding information.

```
PE-1# show ip bgp vpnv4 all tag | begin 10.3.1.7
```

```
   10.3.1.7/32      10.3.1.2
        notag/38

PE-1# show tag-switching forwarding 10.3.1.2
Local  Outgoing   Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC  or Tunnel Id     switched   interface
31     42         10.3.1.2/32
       0          PO3/0/0    point2point
PE-1# show ip cef vrf ospf 10.3.1.7
10.3.1.7/32, version 73, epoch 0, cached adjacency to POS3/0/0
0 packets, 0 bytes
  tag information set
   local tag: VPN-route-head
   fast tag rewrite with PO3/0/0, point2point, tags imposed: {42 38
}
  via 10.3.1.2
, 0 dependencies, recursive
    next hop 10.1.1.17, POS3/0/0 via 10.3.1.2/32
    valid cached adjacency
    tag rewrite with PO3/0/0, point2point, tags imposed: {42 38}
```

If a prefix is learned across the sham-link and the path via the sham-link is selected as the best, the PE router does not generate an MP-BGP update for the prefix. It is not possible to route traffic from one sham-link over another sham-link.

In the following output, PE-2 shows how an MP-BGP update for the prefix is not generated. Although 10.3.1.7/32 has been learned via OSPF across the sham-link as shown in bold, no local generation of a route into BGP is performed. The only entry within the BGP table is the MP-BGP update received from PE-3 (the egress PE router for the 10.3.1.7/32 prefix).

```
PE-2# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100
", distance 110, metric 12, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:00:10 ago
  Routing Descriptor Blocks:
  * 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:00:10 ago
      Route metric is 12, traffic share count is 1
PE-2# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 166
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

The PE router uses the information received from MP-BGP to set the ongoing label stack of incoming packets, and to decide to which egress PE router to label switch the packets.

Example Sham-Link Between Two PE Routers

The following example shows how to configure a sham-link between two PE routers:

```
Router1(config)
# interface loopback 1
Router1(config-if)# ip vrf forwarding ospf
Router1(config-if)# ip address 10.2.1.1 255.255.255.255
!
Router2(config)# interface loopback 1
Router2(config-if)# ip vrf forwarding ospf
Router2(config-if)# ip address 10.2.1.2 255.255.255.255
!
```

```
Router1(config)# router ospf 100 vrf ospf
Router1(config-if)# area 1 sham-link 10.2.1.1 10.2.1.2 cost 40
!
Router2(config)# router ospf 100 vrf ospf
Router2(config-if)# area 1 sham-link 10.2.1.2 10.2.1.1 cost 40
```

Additional References

The following sections provide references related to the OSPF Sham-Link Support for MPLS VPN feature.

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
MPLS Virtual Private Networks	"MPLS Virtual Private Networks"

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
RFC 1163	*A Border Gateway Protocol*
RFC 1164	*Application of the Border Gateway Protocol in the Internet*
RFC 2283	*Multiprotocol Extensions for BGP-4*

RFC	Title
RFC 2328	*Open Shortest Path First, Version 2*
RFC 2547	*BGP/MPLS VPNs*

Technical Assistance

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

Feature Information for OSPF Sham-Link Support for MPLS VPN

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 14: Feature Information for OSPF Sham-Link Support for MPLS VPN

Feature Name	Releases	Feature Information
OSPF Sham-Link Support for MPLS VPN	Cisco IOS XE Release 2.1	This feature allows you to use a sham-link to connect Virtual Private Network (VPN) client sites that run OSPF and share backdoor OSPF links in a Multiprotocol Label Switching (MPLS) VPN configuration. The following commands are introduced or modified in the feature documented in this module: • **area sham-link cost** • **show ip ospf sham-links**

Glossary

BGP --Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined in RFC 1163.

CE router --customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers are not aware of associated VPNs.

CEF -- Cisco Express Forwarding. An advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns.

IGP --Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include IGRP, OSPF, and RIP.

LSA --link-state advertisement. A broadcast packet used by link-state protocols. The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

MPLS --Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

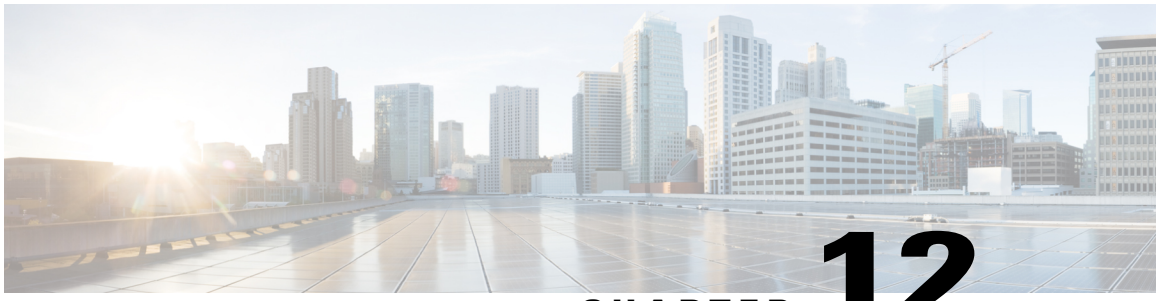
OSPF --Open Shortest Path First protocol.

PE router --provider edge router. A router that is part of a service provider network connected to a customer edge (CE) router. All VPN processing occurs in the PE router.

SPF --shortest path first calculation.

VPN --Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

VRF --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.



CHAPTER 12

OSPF Support for Multi-VRF on CE Routers

The OSPF Support for Multi-VRF on CE Routers feature provides the capability to suppress provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VPN routing and forwarding (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

OSPF multi-VRF allows you to split the router into multiple virtual routers, where each router contains its own set of interfaces, routing table, and forwarding table.

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.

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 Support for Multi-VRF on CE Routers

The OSPF Support for Multi-VRF on CE Routers feature provides the capability to suppress provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets

between the OSPF and BGP protocols. When VPN routing and forwarding (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes.

OSPF multi-VRF allows you to split the router into multiple virtual routers, where each router contains its own set of interfaces, routing table, and forwarding table. OSPF multi-VRF gives you the ability to segment parts of your network and configure those segments to perform specific functions, yet still maintain correct routing information.

How to Configure OSPF Support for Multi-VRF on CE Routers

Configuring the Multi-VRF Capability for OSPF Routing

Before You Begin

CEF must be running on the network.

SUMMARY STEPS

1. **enable**
2. **show ip ospf** [*process-id*
3. **configure terminal**
4. **vpdn- group** *name*
5. **exit**
6. **resource-pool profile vpdn** *name*
7. **vpdn group** *name*
8. **vpn vrf** *vrf-name* | **id** *vpn-id*
9. **exit**
10. **router ospf** *process-id* [**vrf** *vpn-name*]
11. **capability vrf-lite**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf** [*process-id* **Example:** `Router# show ip ospf 1`	Displays the status of the router. If the display indicates that the router is connected to the VPN backbone, you can use the **capability vrf-lite** command to decouple the PE router from the VPN backbone.

	Command or Action	Purpose
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 4	**vpdn- group** *name* **Example:** `Router(config)# vpdn-group mygroup`	Creates a VPDN group.
Step 5	**exit** **Example:** `Router(config-vpdn)# exit`	Leaves the configuration mode and returns to global configuration mode.
Step 6	**resource-pool profile vpdn** *name* **Example:** `Router(config)# resource-pool profile vpdn company1`	Creates a virtual private dialup network (VPDN) profile and enters VPDN profile configuration mode.
Step 7	**vpdn group** *name* **Example:** `Router(config-vpdn-profile)# vpdn group mygroup`	Associates a virtual private dialup network (VPDN) group with a customer or VPDN profile.
Step 8	**vpn vrf** *vrf-name* | **id** *vpn-id* **Example:** `Router(config-vpdn)# vpn vrf grc`	Specifies that the source and destination IPv4 addresses of a given virtual private dialup network (VPDN) group belong to a specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
Step 9	**exit** **Example:** `Router(config-vpdn)# exit`	Leaves the configuration mode and returns to global configuration mode.
Step 10	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 1 vrf grc`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process. • Use the **vrf** keyword and *vpn-name* argument to identify a VPN.

	Command or Action	Purpose
Step 11	**capability vrf-lite** **Example:** `Router(config-router)# capability vrf-lite`	Applies the multi-VRF capability to the OSPF process.

Verifying the OSPF Multi-VRF Configuration

No specific **debug** or **show** commands are associated with this feature. You can verify the success of the OSPF multi-VRF configuration by using the **show ip ospf** *process-id*] command to verify that the router is not connected to the VPN backbone.

This output from the **show ip ospf process**command indicates that the PE router is currently connected to the backbone.

```
Router# show ip ospf 12
 Routing Process "ospf 12" with ID 172.16.1.1 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Connected to MPLS VPN Superbackbone
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 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 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

When the OSPF VRF process is configured with the **capability vrf-lite** command under the **router ospf** command, the "Connected to MPLS VPN Superbackbone" line will not be present in the display.

Configuration Example for OSPF Support for Multi-VRF on CE Routers

Example Configuring the Multi-VRF Capability

This example shows a basic OSPF network with a VRF named grc configured. The **capability vrf-lite** command is entered to suppress the PE checks.

```
!
ip cef
ip vrf grc
 rd 1:1
interface Serial2/0/0
 ip vrf forwarding grc
 ip address 192.168.1.1 255.255.255.252
!
interface Serial3/0/0
```

```
 ip vrf forwarding grc
 ip address 192.168.2.1 255.255.255.252
...
!
router ospf 9000 vrf grc
 log-adjacency-changes
 capability vrf-lite
 redistribute rip metric 1 subnets
 network 192.168.1.0 0.0.0.255 area 0
!
router rip
 address-family ipv4 vrf grc
 redistribute ospf 9000 vrf grc
 network 192.168.2.0
 no auto-summary
 end
Device# show ip route vrf grc
Routing Table: grc
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is not set
O IA 192.168.192.0/24 [110/138] via 192.168.1.13, 00:06:08, Serial2/0/0
                      [110/138] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.242.0/24 [110/74] via 192.168.1.13, 00:06:08, Serial2/0/0
O IA 192.168.193.0/24 [110/148] via 192.168.1.13, 00:06:08, Serial2/0/0
                      [110/148] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.128.0/24 [110/74] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.129.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0/0
O IA 192.168.130.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0/0
     172.16.0.0/24 is subnetted, 2 subnets
O E2    172.16.9.0 [110/5] via 192.168.1.13, 00:06:08, Serial2/0/0
O E2    172.16.10.0 [110/5] via 192.168.1.13, 00:06:08, Serial2/0/0
O IA 192.168.131.0/24 [110/94] via 192.168.1.9, 00:06:20, Serial3/0/0
     192.168.1.0/30 is subnetted, 4 subnets
C       192.168.1.8 is directly connected, Serial3/0/0
C       192.168.1.12 is directly connected, Serial2/0/0
O       192.168.1.0 [110/128] via 192.168.1.9, 00:06:20, Serial3/0/0
O       192.168.1.4 [110/128] via 192.168.1.13, 00:06:20, Serial2/0/0
```

Additional References

For additional information related to OSPF support for multi-VRF on CE routers, see the following references.

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"
Multiprotocol Label Switching (MPLS)	*Cisco IOS XE Multiprotocol Label Switching Configuration Guide, Release 2*
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 software releases , and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

Feature Information for OSPF Support for Multi-VRF on CE Routers

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 15: Feature Information for OSPF Support for Multi-VRF on CE Routers

Feature Name	Releases	Feature Information
OSPF Support for Multi-VRF on CE Routers	Cisco IOS XE Release 2.1 Cisco IOS XE Release 3.1.0 SG	The OSPF Support for Multi-VRF on CE Routers feature provides the capability to suppress provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VPN routing and forwarding (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes. The following commands are introduced or modified in the feature documented in this module: • **capability vrf-lite**

Glossary

CE Router --Customer Edge router, an edge router in the C network, defined as a C router which attaches directly to a P router.

C Network --Customer (enterprise or service provider) network.

C Router --Customer router, a router in the C network.

LSA --link-state advertisement . Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.

PE Router --Provider Edge router, an edge router in the P network, defined as a P router which attaches directly to a C router.

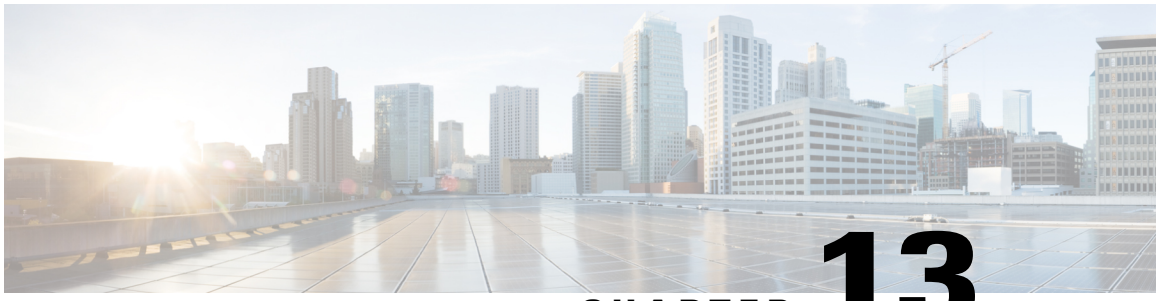
P Network --MPLS-capable service provider core network. P routers perform MPLS.

P Router --Provider router, a router in the P network.

SPF --shortest path first. A routing algorithm that iterates on length of path to determine a shortest-path spanning tree.

VPN --Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another.

VRF --VPN Routing and Forwarding.



CHAPTER 13

OSPFv2 Multiarea Adjacency

This module describes how to configure multiarea adjacency for Open Shortest Path First version 2 (OSPFv2). You can add more than one area to an existing OSPFv2 primary interface. The additional logical interfaces support multiarea adjacency.

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.

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 Multiarea Adjacency

- Ensure that Open Shortest Path First (OSPF) is configured on the primary interface.
- Ensure that the primary interface type is point-to-point.

Restrictions for OSPFv2 Multiarea Adjacency

A multiarea interface has the following restrictions.

- Operates only if OSPF is configured on the primary interface.
- Exists as a logical construct over a primary interface for OSPF; however, the neighbor state on the primary interface is independent of the multiarea interface.
- Establishes a neighbor relationship with the corresponding multiarea interface on the neighboring device. A mixture of multiarea and primary interfaces is not supported.
- Advertises an unnumbered point-to-point link in the device link-state advertisement (LSA) for the corresponding area when the neighbor state is full.
- Inherits all the OSPF parameters (such as, authentication) from the primary interface. You cannot configure the parameters on a multiarea interface; however, you can configure the parameters on the primary interface.

Information About OSPFv2 Multiarea Adjacency

OSPFv2 Multiarea Adjacency Overview

The Open Shortest Path First (OSPF) protocol allows you to divide a network topology into separate areas. The interface on which OSPF is configured belongs to only one area at any given point of time. This causes suboptimal routing for certain topologies, due to intra-area route preference over the interarea routes.

Open Shortest Path First version 2 (OSPFv2) allows a single physical link to be shared by multiple areas. This creates an intra-area path in each of the corresponding areas sharing the same link. All areas have an interface on which OSPF is configured. One of these interfaces is designated as the primary interface and others as secondary interfaces.

The OSPFv2 Multiarea Adjacency feature allows you to configure a link on the primary interface to enable optimized routing in multiple areas. Each multiarea interface is announced as a point-to-point unnumbered link. The multiarea interface exists as a logical construct over an existing primary interface. The neighbor state on the primary interface is independent of the neighbor state of the multiarea interface. The multiarea interface establishes a neighbor relationship with the corresponding multiarea interface on the neighboring device. You can only configure multiarea adjacency on an interface that has two OSPF speakers. In case of native broadcast networks, the interface must be configured as an OSPF point-to-point type to enable the interface for multiarea adjacency.

Use the **ip ospf multi-area** command to configure multiarea adjacency on the primary OSPFv2 interface.

How to Configure OSPFv2 Multiarea Adjacency

Configuring OSPFv2 Multiarea Adjacency

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **ip ospf** *proces-id* **area** *area-id*
6. **ip ospf network point-to-point**
7. **ip ospf multi-area** *multi-area-id*
8. **ip ospf multi-area** *multi-area-id* **cost** *interface-cost*
9. **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	**interface** *type number* **Example:** `Device(config)# interface Ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Device(config)# ip address 10.0.12.1 255.255.255.0`	Assigns an IP address to this interface.
Step 5	**ip ospf** *proces-id* **area** *area-id* **Example:** `Device (config-if)# ip ospf 10 area 8`	Configures the primary OSPF interface. • The *process-id* argument identifies the OSPF process. The range is from 1 to 65535.

	Command or Action	Purpose
		• The *area-id* argument identifies the OSPF area. The range is from 0 to 4294967295, or you can use an IP address.
Step 6	**ip ospf network point-to-point** **Example:** `Device (config-if)# ip ospf network point-to-point`	Specifies the primary interface type as point-to-point.
Step 7	**ip ospf multi-area** *multi-area-id* **Example:** `Device (config-if)# ip ospf multi-area 11`	Configures multiarea adjacency on the interface. • The *multi-area-id* argument identifies the OSPF multiarea. The range is from 0 to 4294967295, or you can use an IP address.
Step 8	**ip ospf multi-area** *multi-area-id* **cost** *interface-cost* **Example:** `Device (config-if)# ip ospf multi-area 11 cost 10`	(Optional) Specifies the cost of sending a packet on an Open Shortest Path First (OSPF) multiarea interface,
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv2 Multiarea Adjacency

Example: Configuring OSPFv2 Multiarea Adjacency

```
Device# enable
Device# configure terminal
Device(config)# interface Ethernet 0/0
Device (config-if)# ip address 10.0.12.1 255.255.255.0
Device (config-if)# ip ospf 1 area 0
Device (config-if)# ip ospf network point-to-point
Device (config-if)# ip ospf multi-area 2
Device (config-if)# ip ospf multi-area 2 cost 10
Device (config-if)# end
```

The following is a sample output from the **show ip ospf 2 multi-area** command.

```
Device# show ip ospf 2 multi-area

OSPF_MA1 is up, line protocol is up
  Primary Interface Ethernet0/0, Area 2
  Interface ID 2
  MTU is 1500 bytes
  Neighbor Count is 1
```

The following is a sample output from the **show ip ospf interface** command.

```
Device# show ip ospf interface

Ethernet0/0 is up, line protocol is up
  Internet Address 10.0.12.1/24, Area 0, Attached via Interface Enable
  Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  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 10.0.0.1
  Suppress hello for 0 neighbor(s)
  Multi-area interface Count is 1
    OSPF_MA1 interface exists in area 2 Neighbor Count is 1
OSPF_MA1 is up, line protocol is up
  Interface is unnumbered. Using address of Ethernet0/0 (10.0.12.1), Area 2, Attached via
Multi-area
  Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Can be protected by per-prefix Loop-Free FastReroute
  Can be used for per-prefix Loop-Free FastReroute repair paths
  Index 1/3, flood queue length 0
  Next 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
  Suppress hello for 0 neighbor(s)
```

Additional References for OSPFv2 Multiarea Adjacency

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Protocol-independent features that work with OSPF	“Configuring IP Routing Protocol-Independent Features” module

RFCs

RFC	Title
RFC 5185	*OSPF Multi-Area Adjacency*, May 2008

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

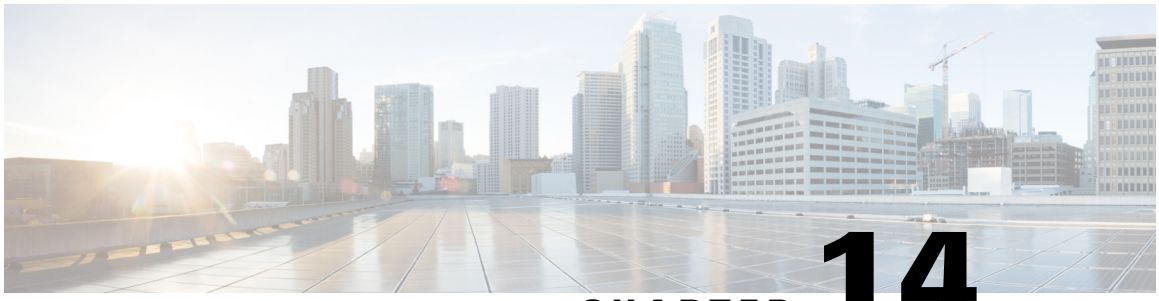
Feature Information for OSPFv2 Multiarea Adjacency

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 16: Feature Information for OSPFv2 Multiarea Adjacency

Feature Name	Releases	Feature Information
OSPFv2 Multiarea Adjacency	Cisco IOS XE Release 3.10S	OSPFv2 multiarea adjacency allows you to configure a link on the primary interface in multiple OSPF areas to enable optimized routing. The following commands were introduced or modified: **ip ospf multi-area**, **ip ospf multi-area cost**, and **show ip ospf multi-area**.



CHAPTER 14

OSPFv2 Autoroute Exclude

The OSPFv2 Autoroute Exclude feature allows specific destinations and prefixes to avoid Traffic Engineering (TE) tunnels for the packet transport. The rest of the prefixes can still be set to use TE tunnels. Prefixes that are excluded do not use a TE tunnel path. Only native non-TE paths are downloaded to RIB for such routes. This module describes how to configure the OSPFv2 Autoroute Exclude feature.

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.

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 Autoroute Exclude

- Open Shortest Path First (OSPF) must be configured in your network.
- Cisco Express Forwarding (CEF) must be enabled.
- Multiprotocol Label Switching (MPLS) TE tunnels must be configured.

Information About OSPFv2 Autoroute Exclude

Overview of OSPFv2 Autoroute Exclude

The Autoroute feature is an IP routing method that forces OSPF to use MPLS TE tunnels to build paths for IP traffic routes.

The Autoroute feature enables all routes to use TE Tunnels, even if there is an alternate non-TE path available for that route.

The OSPFv2 Autoroute Exclude feature allows specific destinations or prefixes to avoid TE tunnels, while other prefixes can still be configured to use TE tunnels. Prefixes that are excluded do not use a TE tunnel path. Only native non-TE paths are downloaded to RIB for such routes.

The auto route exclude option is configured under the router OSPF configuration mode by using a prefix list. IP addresses and prefixes that are members of this prefix list are excluded from TE tunnels, even when the auto route is enabled on them. If the IP addresses or prefixes are added to the prefix list, they are dynamically routed without passing through the TE tunnel. If the IP addresses or prefixes are removed from the prefix list, they are dynamically rerouted back on the TE tunnel path.

How to Configure OSPFv2 Autoroute Exclude

Configuring OSPFv2 Autoroute Exclude

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-ID*
4. **router-id** *ip-address*
5. **mpls traffic-eng router-id** *interface-name*
6. **mpls traffic-eng area***number*
7. **mpls traffic-eng autoroute-exclude prefix-list** *prefix-list-name*
8. **exit**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-ID* **Example:** `Device(config)# router ospf 18`	Configures OSPF routing process and enters OSPF router configuration mode.
Step 4	**router-id** *ip-address* **Example:** `Device(config-router)# router-id 10.1.1.1`	Enables to use a fixed router ID in router configuration mode.
Step 5	**mpls traffic-eng router-id** *interface-name* **Example:** `Device(config-router)# mpls traffic-eng router-id Loopback0`	Specifies the traffic engineering router identifier for the node and the IP address associated with a given interface.
Step 6	**mpls traffic-eng area***number* **Example:** `Device(config-router)# mpls traffic-eng area 0`	Configures a router running OSPF MPLS so that it floods traffic engineering for the indicated OSPF area.
Step 7	**mpls traffic-eng autoroute-exclude prefix-list** *prefix-list-name* **Example:** `Device(config-router)# mpls traffic-eng autoroute-exclude prefix-list kmd`	Allows specific destinations and prefixes to avoid routing through TE tunnels. • Prefixes that are excluded do not use a TE tunnel path.
Step 8	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv2 Autoroute Exclude

Example: Configuring OSPFv2 Autoroute Exclude

```
!
router ospf 1
```

```
 router-id 3.3.3.3
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng autoroute-exclude prefix-list XX

!
```

Additional References for OSPFv2 Autoroute Exclude

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF	*IP Routing: OSPF Configuration Guide*
Configuring Basic Cisco Express Forwarding	*IP Switching: Cisco Express Forwarding Configuration Guide*
MPLS Traffic Engineering Tunnel Source	*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

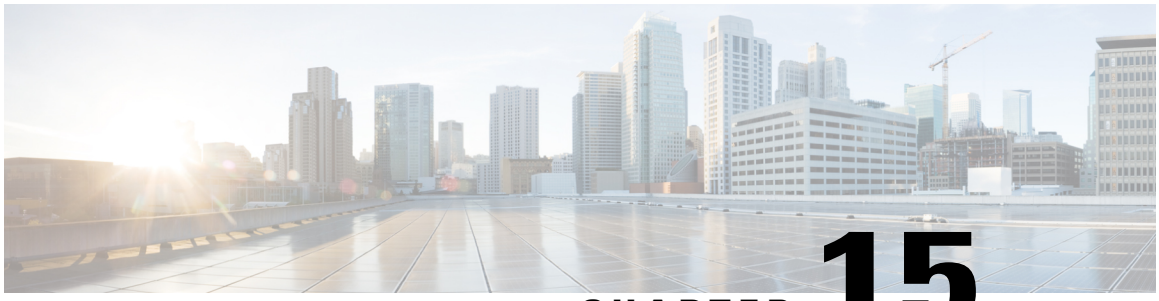
Feature Information for OSPFv2 Autoroute Exclude

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 17: Feature Information for OSPFv2 Autoroute Exclude

Feature Name	Releases	Feature Information
OSPFv2 Autoroute Exclude	Cisco IOS XE 3.13S	The OSPFv2 Autoroute Exclude feature allows specific destinations and prefixes to avoid TE tunnels for the packet transport. The following commands were introduced or modified: **mpls traffic-eng autoroute-exclude prefix list**.



CHAPTER 15

OSPFv3 Address Families

The Open Shortest Path First version 3 (OSPFv3) address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may have two processes per interface, but only one process per address family (AF).

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.

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 OSPFv3 Address Families

- To use the IPv4 unicast address families (AF) in OSPFv3, you must enable IPv6 on a link, although the link may not be participating in IPv6 unicast AF.
- With the OSPFv3 Address Families feature, users may have two processes per interface, but only one process per AF. If the AF is IPv4, an IPv4 address must first be configured on the interface, but IPv6 must be enabled on the interface.

Information About OSPFv3 Address Families

OSPFv3 Address Families

The OSPFv3 address families feature enables both IPv4 and IPv6 unicast traffic to be supported. With this feature, users may have two processes per interface, but only one process per AF. If the IPv4 AF is used, an IPv4 address must first be configured on the interface, but IPv6 must be enabled on the interface. A single IPv4 or IPv6 OSPFv3 process running multiple instances on the same interface is not supported.

Users with an IPv6 network that uses OSPFv3 as its IGP may want to use the same IGP to help carry and install IPv4 routes. All devices on this network have an IPv6 forwarding stack. Some (or all) of the links on this network may be allowed to do IPv4 forwarding and be configured with IPv4 addresses. Pockets of IPv4-only devices exist around the edges running an IPv4 static or dynamic routing protocol. In this scenario, users need the ability to forward IPv4 traffic between these pockets without tunneling overhead, which means that any IPv4 transit device has both IPv4 and IPv6 forwarding stacks (e.g., is dual stack).

This feature allows a separate (possibly incongruent) topology to be constructed for the IPv4 AF. It installs IPv4 routes in IPv4 RIB, and then the forwarding occurs natively. The OSPFv3 process fully supports an IPv4 AF topology and can redistribute routes from and into any other IPv4 routing protocol.

An OSPFv3 process can be configured to be either IPv4 or IPv6. The **address-family** command is used to determine which AF will run in the OSPFv3 process, and only one address family can be configured per instance. Once the AF is selected, users can enable multiple instances on a link and enable address-family-specific commands.

Different instance ID ranges are used for each AF. Each AF establishes different adjacencies, has a different link state database, and computes a different shortest path tree. The AF then installs the routes in AF-specific RIB. LSAs that carry IPv6 unicast prefixes are used without any modification in different instances to carry each AFs' prefixes.

The IPv4 subnets configured on OSPFv3-enabled interfaces are advertised through intra-area prefix LSAs, just as any IPv6 prefixes. External LSAs are used to advertise IPv4 routes redistributed from any IPv4 routing protocol, including connected and static. The IPv4 OSPFv3 process runs the SPF calculations and finds the shortest path to those IPv4 destinations. These computed routes are then inserted in the IPv4 RIB (computed routes are inserted into an IPv6 RIB for an IPv6 AF).

Because the IPv4 OSPFv3 process allocates a unique pdbindex in the IPv4 RIB, all other IPv4 routing protocols can redistribute routes from it. The parse chain for all protocols is same, so the **ospfv3** keyword added to the list of IPv4 routing protocols causes OSPFv3 to appear in the **redistribute** command from any IPv4 routing protocol. With the **ospfv3** keyword, IPv4 OSPFv3 routes can be redistributed into any other IPv4 routing protocol as defined in the **redistribute ospfv3** command.

Third-party devices will not neighbor with devices running the AF feature for the IPv4 AF because they do not set the AF bit. Therefore, those devices will not participate in the IPv4 AF SPF calculations and will not install the IPv4 OSPFv3 routes in the IPv6 RIB.

How to Configure OSPFv3 Address Families

Configuring the OSPFv3 Router 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 perform 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.

	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	**area** *area-ID* [**default-cost** | **nssa** | **stub**] **Example:** `Device(config-router)# area 1`	Configures the OSPFv3 area.
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.

	Command or Action	Purpose
Step 10	**log-adjacency-changes** [**detail**] **Example:** `Device(config-router)# log-adjacency-changes`	Configures the router 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 using an IPv4 OSPFv3 process.
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`	Use a fixed device ID.

Configuring the IPv6 Address Family in OSPFv3

Perform this task to configure the IPv6 address family in OSPFv3. Once you have completed step 4 and entered IPv6 address-family configuration mode, you can perform any of the subsequent steps in this task as needed to configure the IPv6 AF.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **area** *area-ID* **range** *ipv6-prefix* / *prefix-length*
6. **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*]
7. **default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value*| **route-map** *map-name*]
8. default-metric *metric-value*
9. **distance** *distance*
10. **distribute-list prefix-list** *list-name* {**in**[*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
11. **maximum-paths** *number-paths*
12. **summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*]

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 ospfv3** [*process-id*] **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**address-family ipv6 unicast** **Example:** **Example:** `or`	Enters IPv6 address family configuration mode for OSPFv3. or Enters IPv4 address family configuration mode for OSPFv3.

	Command or Action	Purpose

	Example:
	address-family ipv4
	unicast
	Example:
	`Router(config-router)# address-family ipv6 unicast`
	Example:
	Example:
	`or`
	Example:
	`Router(config-router)# address-family ipv4 unicast`	

Step 5	**area** *area-ID* **range** *ipv6-prefix* / *prefix-length* **Example:** `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	Configures OSPFv3 area parameters.
Step 6	**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:** `Router(config-router-af)# default area 1`	Returns an OSPFv3 parameter to its default value.
Step 7	**default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value*| **route-map** *map-name*] **Example:** `Router(config-router-af)# default-information originate always metric 100 metric-type 2`	Generates a default external route into an OSPFv3 for a routing domain.

	Command or Action	Purpose
Step 8	default-metric *metric-value* **Example:** `Router(config-router-af)# default-metric 10`	Sets default metric values for IPv4 and IPv6 routes redistributed into the OSPFv3 routing protocol.
Step 9	**distance** *distance* **Example:** `Router(config-router-af)# distance 200`	Configures an administrative distance for OSPFv3 routes inserted into the routing table.
Step 10	**distribute-list prefix-list** *list-name* {**in**[*interface-type interface-number*] | **out** *routing-process* [*as-number*]} **Example:** `Router(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	Applies a prefix list to OSPFv3 routing updates that are received or sent on an interface.
Step 11	**maximum-paths** *number-paths* **Example:** `Router(config-router-af)# maximum-paths 4`	Controls the maximum number of equal-cost routes that a process for OSPFv3 routing can support.
Step 12	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] **Example:** `Router(config-router-af)# summary-prefix FEC0::/24`	Configures an IPv6 summary prefix in OSPFv3.

Configuring the IPv4 Address Family in OSPFv3

Perform this task to configure the IPv4 address family in OSPFv3. Once you have completed step 4 and entered IPv4 address-family configuration mode, you can perform any of the subsequent steps in this task as needed to configure the IPv4 AF.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv4 unicast**
5. **area** *area-id* **range** *ip-address ip-address-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
6. **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*]
7. **default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value*| **route-map** *map-name*]
8. default-metric *metric-value*
9. **distance** *distance*
10. **distribute-list prefix-list** *list-name* {**in**[*interface-type interface-number*] | **out** *routing-process* [*as-number*]}
11. **maximum-paths** *number-paths*
12. **summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*]

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 OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**address-family ipv4 unicast** **Example:** `Device(config-router)# address-family ipv4 unicast`	Enters IPv4 address family configuration mode for OSPFv3.

	Command or Action	Purpose
Step 5	**area** *area-id* **range** *ip-address ip-address-mask* [**advertise** | **not-advertise**] [**cost** *cost*] **Example:** `Device(config-router-af)# area 0 range 192.168.110.0 255.255.0.0`	Consolidates and summarizes routes at an area boundary.
Step 6	**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-af)# default area 1`	Returns an OSPFv3 parameter to its default value.
Step 7	**default-information originate** [**always** | **metric** *metric-value* | **metric-type** *type-value*| **route-map** *map-name*] **Example:** `Device(config-router-af)# default-information originate always metric 100 metric-type 2`	Generates a default external route into an OSPFv3 for a routing domain.
Step 8	default-metric *metric-value* **Example:** `Device(config-router-af)# default-metric 10`	Sets default metric values for IPv4 and IPv6 routes redistributed into the OSPFv3 routing protocol.
Step 9	**distance** *distance* **Example:** `Device(config-router-af)# distance 200`	Configures an administrative distance for OSPFv3 routes inserted into the routing table.
Step 10	**distribute-list prefix-list** *list-name* {**in**[*interface-type interface-number*] | **out** *routing-process* [*as-number*]} **Example:** `Device(config-router-af)# distribute-list prefix-list PL1 in Ethernet0/0`	Applies a prefix list to OSPFv3 routing updates that are received or sent on an interface.
Step 11	**maximum-paths** *number-paths* **Example:** `Device(config-router-af)# maximum-paths 4`	Controls the maximum number of equal-cost routes that a process for OSPFv3 routing can support.

	Command or Action	Purpose
Step 12	**summary-prefix** *prefix* [**not-advertise** | **tag** *tag-value*] **Example:** `Device(config-router-af)# summary-prefix FEC0::/24`	Configures an IPv6 summary prefix in OSPFv3.

Configuring Route Redistribution in OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **redistribute** source-*protocol* [*process-id*] [*options*]

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 ospfv3** [*process-id*] **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**address-family ipv6 unicast** **Example:**	Enters IPv6 address family configuration mode for OSPFv3. or Enters IPv4 address family configuration mode for OSPFv3.

	Command or Action	Purpose

	Example:
	or
	Example:
	address-family ipv4
	unicast
	Example:
	`Router(config-router)# address-family ipv6 unicast`
	Example:
	Example:
	or
	Example:
	`Router(config-router)# address-family ipv4 unicast`	

Step 5	**redistribute** source-*protocol* [*process-id*] [*options*] **Example:**	Redistributes IPv6 and IPv4 routes from one routing domain into another routing domain.

Enabling OSPFv3 on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ospfv3** *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*]
   - **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-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	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	Do one of the following: • **ospfv3** *process-id* **area** *area-ID* {**ipv4** | **ipv6**} [**instance** *instance-id*] • **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*] **Example:** `Device(config-if)# ospfv3 1 area 1 ipv4`	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF. or Enables OSPFv3 on an interface.

	Command or Action	Purpose
	Example: `Device(config-if)# ipv6 ospf 1 area 0`	

Defining an OSPFv3 Area Range for the IPv6 or IPv4 Address Family

The cost of the summarized routes will be the highest cost of the routes being summarized. For example, if the following routes are summarized:

```
OI  2001:DB8:0:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
OI  2001:DB8:0:8::/64 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
OI  2001:DB8:0:9::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
```

They become one summarized route, as follows:

```
OI  2001:DB8::/48 [110/100]
     via FE80::A8BB:CCFF:FE00:6F00, GigabitEthernet0/0/0
```

Before You Begin

OSPFv3 routing must be enabled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **address-family ipv6 unicast**
5. **area** *area-ID* **range** *ipv6-prefix*

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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** [*process-id*] **Example:** `Router(config)# router ospfv3 1`	Enables OSPFv3 router configuration mode for the IPv4 or IPv6 address family.

Step 4	**address-family ipv6 unicast**
	Example:
	Example:
	or
	Example:
	address-family ipv4
	unicast
	Example:
	`Router(config-router)# address-family ipv6 unicast`
	Example:
	Example:
	or
	Example:
	`Router(config-router)# address-family ipv4 unicast`
		Enters IPv6 address family configuration mode for OSPFv3.
		or
		Enters IPv4 address family configuration mode for OSPFv3.

Step 5	**area** *area-ID* **range** *ipv6-prefix* **Example:** `Router(config-router-af)# area 1 range 2001:DB8:0:0::0/128`	Configures OSPFv3 area parameters.

Defining an OSPFv3 Area Range

This task can be performed in releases prior to Cisco IOS XE Release 3.4S.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **area** *area-id* **range** *ipv6-prefix* / *prefix-length* **advertise** | **not-advertise**] [**cost** *cost*]

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	**ipv6 router ospf** *process-id* **Example:** `Router(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**area** *area-id* **range** *ipv6-prefix* / *prefix-length* **advertise** | **not-advertise**] [**cost** *cost*] **Example:** `Router(config-rtr)# area 1 range 2001:DB8::/48`	Consolidates and summarizes routes at an area boundary.

Configuration Examples for OSPFv3 Address Families

Example: Configuring OSPFv3 Address Families

```
Device# show ospfv3
 Routing Process "ospfv3 1" with ID 10.0.0.1
 Supports IPv6 Address Family
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 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 0. Checksum Sum 0x000000
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 Graceful restart helper support enabled
 Reference bandwidth unit is 100 mbps
 Relay willingness value is 128
 Pushback timer value is 2000 msecs
 Relay acknowledgement timer value is 1000 msecs
 LSA cache Disabled : current count 0, maximum 1000
 ACK cache Disabled : current count 0, maximum 1000
 Selective Peering is not enabled
 Hello requests and responses will be sent multicast
```

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
OSPFv3 Address Families	" *OSPF Forwarding Address Suppression in Translated Type-5 LSAs* " 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 OSPFv3 Address Families

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.

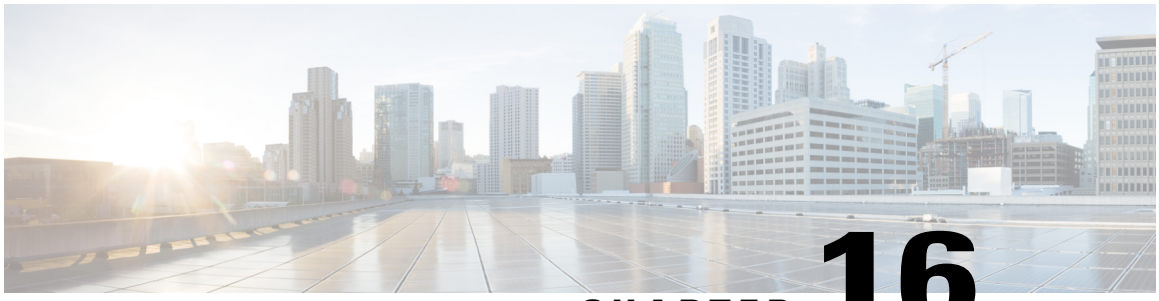
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 18: Feature Information for OSPFv3 Address Families

Feature Name	Releases	Feature Information
OSPFv3 Address Families	Cisco IOS XE Release 3.4S	

Feature Name	Releases	Feature Information
		The OSPFv3 address families feature enables IPv4 and IPv6 unicast traffic to be supported with a single network topology. The following commands were introduced or modified: **address-family ipv4 (OSPFv3)**, **address-family ipv6 (OSPFv3)**, **area (OSPFv3)**, **auto-cost (OSPFv3)**, **bfd all-interfaces (OSPFv3)**, **clear ospfv3 counters**, **clear ospfv3 force-spf**, **clear ospfv3 process**, **clear ospfv3 redistribution**, **clear ospfv3 traffic**, **debug ospfv3**, **debug ospfv3 database-timer rate-limit**, **debug ospfv3 events**, **debug ospfv3 lsdb**, **debug ospfv3 packet**, **debug ospfv3 spf statistic**, **default (OSPFv3)**, **default-information originate (OSPFv3)**, **default-metric (OSPFv3)**, **distance (OSPFv3)**, **distribute-list prefix-list (OSPFv3)**, **event-log (OSPFv3)**, **log-adjacency-changes (OSPFv3)**, **maximum-paths (OSPFv3)**, **ospfv3 area**, **ospfv3 authentication**, **ospfv3 bfd**, **ospfv3 cost**, **ospfv3 database-filter**, **ospfv3 dead-interval**, **ospfv3 demand-circuit**, **ospfv3 encryption**, **ospfv3 flood-reduction**, **ospfv3 hello-interval**, **ospfv3 mtu-ignore**, **ospfv3 network**, **ospfv3 priority**, **ospfv3 retransmit-interval**, **ospfv3 transmit-delay**, **passive-interface (OSPFv3)**, **queue-depth (OSPFv3)**, **redistribute (OSPFv3)**, **router ospfv3**, **router-id (OSPFv3)**, **show ospfv3 border-routers**, **show ospfv3 database**, **show ospfv3 events**, **show ospfv3 flood-list**, **show ospfv3 graceful-restart**, **show ospfv3 interface**, **show ospfv3 max-metric**, **show ospfv3**

Feature Name	Releases	Feature Information
		neighbor, **show ospfv3 request-list**, **show ospfv3 retransmission-list**, **show ospfv3 statistics**, **show ospfv3 summary-prefix**, **show ospfv3 timers rate-limit**, **show ospfv3 traffic**, **show ospfv3 virtual-links**, **summary-prefix (OSPFv3)**, **timers pacing flood (OSPFv3)**, **timers pacing lsa-group (OSPFv3)**, **timers pacing retransmission (OSPFv3)**.



CHAPTER 16

OSPFv3 Authentication Trailer

The OSPFv3 Authentication Trailer feature as specified in RFC 6506 provides a mechanism to authenticate Open Shortest Path First version 3 (OSPFv3) protocol packets as an alternative to existing OSPFv3 IPsec authentication.

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.

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 OSPFv3 Authentication Trailer

Overview of OSPFv3 Authentication Trailer

Prior to the OSPFv3 Authentication Trailer, OSPFv3 IPsec as defined in RFC 4552 was the only mechanism for authenticating protocol packets. The OSPFv3 Authentication Trailer feature defines an alternative mechanism to authenticate OSPFv3 protocol packets that additionally provides a packet replay protection via sequence number and does not have any platform dependencies.

To perform non-IPsec cryptographic authentication, OSPFv3 devices append a special data block, that is, Authentication Trailer, to the end of the OSPFv3 packets. The length of the Authentication Trailer is not included in the length of the OSPFv3 packet but is included in the IPv6 payload length. The Link-Local Signaling (LLS) block is established by the L-bit setting in the "OSPFv3 Options" field in OSPFv3 hello and database description packets. If present, the LLS data block is included along with the OSPFv3 packet in the cryptographic authentication computation.

A new Authentication Trailer (AT)-bit is introduced into the OSPFv3 Options field. OSPFv3 devices must set the AT-bit in OSPFv3 Hello and Database Description packets to indicate that all the packets on this link will include an Authentication Trailer. For OSPFv3 Hello and Database Description packets, the AT-bit indicates the AT is present. For other OSPFv3 packet types, the OSPFv3 AT-bit setting from the OSPFv3 Hello/Database Description setting is preserved in the OSPFv3 neighbor data structure. OSPFv3 packet types that do not include an OSPFv3 Options field will use the setting from the neighbor data structure to determine whether or not the AT is expected. The AT-bit must be set in all OSPFv3 Hello and Database Description packets that contain an Authentication Trailer.

To configure the Authentication Trailer, OSPFv3 utilizes existing Cisco IOS **key chain** command. For outgoing OSPFv3 packets, the following rules are used to select the key from the key chain:

- Select the key that is the last to expire.
- If two keys have the same stop time, select the one with the highest key ID.

The security association (SA) ID maps to the authentication algorithm and the secret key, which is used to generate and verify the message digest. If the authentication is configured but the last valid key is expired, then the packets are sent using the key. A syslog message is also generated. If no valid key is available then the packet is sent without the authentication trailer. When packets are received, the key ID is used to look up the data for that key. If the key ID is not found in the key chain or if the SA is not valid, the packet is dropped. Otherwise, the packet is verified using the algorithm and the key that is configured for the key ID. Key chains support rollover using key lifetimes. A new key can be added to a key chain with the send start time set in the future. This setting allows the new key to be configured on all devices before the keys are actually used.

The hello packets have higher priority than any other OSPFv3 packets and therefore can get re-ordered on the outgoing interface. This reordering can create problems with sequence number verification on neighboring devices. To prevent sequence mismatch, OSPFv3 verifies the sequence number separately for each packet type.

See RFC 6506 for more details on the authentication procedure.

How to Configure OSPFv3 Authentication Trailer

Configuring OSPFv3 Authentication Trailer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ospfv3** [*pid*] [**ipv4** | **ipv6**] **authentication** {**key-chain** *chain-name* | **null**}
5. **router ospfv3** [*process-id*]
6. **address-family ipv6 unicast vrf** *vrf-name*
7. **area** *area-id* **authentication** {**key-chain** *chain-name* | **null**}
8. **area** *area-id* **virtual-link** *router-id* **authentication key-chain** *chain-name*
9. **area** *area-id* **sham-link** *source-address destination-address* **authentication key-chain** *chain-name*
10. **authentication mode** {**deployment** | **normal**}
11. **end**
12. **show ospfv3 interface**
13. **show ospfv3 neighbor** [*detail*]
14. **debug ospfv3 vrf authentication**

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 GigabitEthernet 2/0`	Specifies the interface type and number.
Step 4	**ospfv3** [*pid*] [**ipv4** | **ipv6**] **authentication** {**key-chain** *chain-name* | **null**} **Example:** `Device(config-if)# ospfv3 1 ipv4 authentication key-chain ospf-1`	Specifies the authentication type for an OSPFv3 instance.

	Command or Action	Purpose
Step 5	**router ospfv3** [*process-id*] **Example:** `Device(config-if)# router ospfv3 1`	Enters OSPFv3 router configuration mode.
Step 6	**address-family ipv6 unicast vrf** *vrf-name* **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Configures the IPv6 address family in the OSPFv3 process and enters IPv6 address family configuration mode.
Step 7	**area** *area-id* **authentication** {**key-chain** *chain-name* | **null**} **Example:** `Device(config-router-af)# area 1 authentication key-chain ospf-chain-1`	Configures the authentication trailer on all interfaces in the OSPFv3 area.
Step 8	**area** *area-id* **virtual-link** *router-id* **authentication key-chain** *chain-name* **Example:** `Device(config-router-af)# area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1`	Configures the authentication for virtual links.
Step 9	**area** *area-id* **sham-link** *source-address destination-address* **authentication key-chain** *chain-name* **Example:** `Device(config-router-af)# area 1 sham-link 1.1.1.1 1.1.1.0 authentication key-chain ospf-chain-1`	Configures the authentication for sham links.
Step 10	**authentication mode** {**deployment** | **normal**} **Example:** `Device(config-router-af)# authentication mode deployment`	Specifies the type of authentication used for the OSPFv3 instance. • The **deployment** keyword provides adjacency between configured and unconfigured authentication devices.
Step 11	**end** **Example:** `Device(config-router-af)# end`	Exits IPv6 address family configuration mode and returns to privileged EXEC mode.
Step 12	**show ospfv3 interface** **Example:** `Device# show ospfv3`	(Optional) Displays OSPFv3-related interface information.
Step 13	**show ospfv3 neighbor** [*detail*] **Example:** `Device# show ospfv3 neighbor detail`	(Optional) Displays OSPFv3 neighbor information on a per-interface basis.

	Command or Action	Purpose
Step 14	**debug ospfv3 vrf authentication** **Example:** `Device# debug ospfv3 vrf authentication`	(Optional) Displays debugging information for OSPFv3.

Configuration Examples for OSPFv3 Authentication Trailer

Example: Configuring OSPFv3 Authentication Trailer

```
interface GigabitEthernet 0/0
 ospfv3 1 ipv4 authentication key-chain ospf-1
 router ospfv3 1
  address-family ipv6 unicast vrf vrf1
   area 1 authentication key-chain ospf-1
   area 1 virtual-link 1.1.1.1 authentication key-chain ospf-1
   area 1 sham-link 1.1.1.1 authentication key-chain ospf-1
   authentication mode deployment
!
key chain ospf-1
key 1
   key-string ospf
   cryptographic-algorithm hmac-sha-512
!
```

Example: Verifying OSPFv3 Authentication Trailer

The following examples show the output of the **show ospfv3** commands.

```
Device# show ospfv3
 OSPFv3 1 address-family ipv6
 Router ID 1.1.1.1
...
RFC1583 compatibility enabled
 Authentication configured with deployment key lifetime
 Active Key-chains:
  Key chain mama: Send key 1, Algorithm HMAC-SHA-256, Number of interfaces 1
    Area BACKBONE(0)

Device# show ospfv3 neighbor detail

OSPFv3 1 address-family ipv6 (router-id 2.2.2.2)

 Neighbor 1.1.1.1
    In the area 0 via interface GigabitEthernet0/0
    Neighbor: interface-id 2, link-local address FE80::A8BB:CCFF:FE01:2D00
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.2.2.2 BDR is 1.1.1.1
    Options is 0x000413 in Hello (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Options is 0x000413 in DBD (V6-Bit, E-Bit, R-Bit, AT-Bit)
    Dead timer due in 00:00:33
```

```
    Neighbor is up for 00:05:07
    Last packet authentication succeed
    Index 1/1/1, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec


Device# show ospfv3 interface

GigabitEthernet0/0 is up, line protocol is up
...
  Cryptographic authentication enabled
    Sending SA: Key 25, Algorithm HMAC-SHA-256 - key chain ospf-keys
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Additional References for OSPFv3 Authentication Trailer

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF features	IP Routing: OSPF Configuration Guide

Standards and RFCs

Related Topic	Document Title
RFC for Supporting Authentication Trailer for OSPFv3	RFC 6506
RFC for Authentication/Confidentiality for OSPFv3	RFC 4552

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

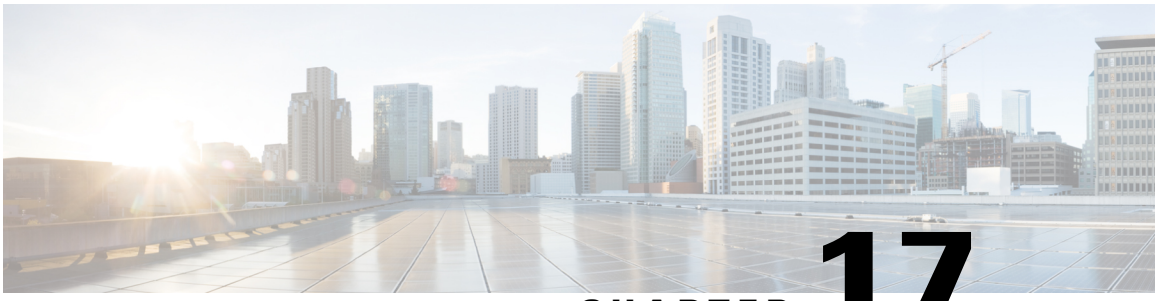
Feature Information for OSPFv3 Authentication Trailer

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 19: Feature Information for OSPFv3 Authentication Trailer

Feature Name	Releases	Feature Information
OSPFv3 Authentication Trailer	Cisco IOS XE Release 3.11S	The OSPFv3 Authentication Trailer feature as specified in RFC 6506 provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication. The following commands were introduced or modified: **ospfv3 authentication key-chain**, **authentication mode**, **debug ospfv3 vrf authentication**.



CHAPTER 17

Autoroute Announce and Forwarding Adjacencies For OSPFv3

The Autoroute Announce and Forwarding Adjacencies for OSPFv3 feature advertises IPv6 routes over MPLS/TE IPv4 tunnels. This module describes how to configure the Autoroute Announce and Forwarding Adjacencies for OSPFv3 feature.

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.

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 Autoroute Announce and Forwarding Adjacencies For OSPFv3

- OSPFv3 must be configured in your network.
- Cisco Express Forwarding (CEF) must be enabled.
- MPLS/TE tunnels must be configured.

Restrictions for Autoroute Announce and Forwarding Adjacencies For OSPFv3

- Autoroute announce and forwarding adjacency cannot be configured together in a same interface.
- When an autoroute announce is used, OSPFv3 does not advertise the tunnel.
- When forwarding adjacencies are used, OSPFv3 advertises the tunnel link in an LSA.

Information About Autoroute Announce and Forwarding Adjacencies For OSPFv3

Overview of Autoroute Announce and Forwarding Adjacencies For OSPFv3

The OSPFv3 support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels feature adds OSPFv3 support to the Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) tunnels feature, which allows a network administrator to handle a traffic engineering, MPLS tunnel as a link in an Interior Gateway Protocol (IGP) network based on the shortest path first (SPF) algorithm. An OSPFv3 forwarding adjacency can be created between routers in the same area.

OSPFv3 includes MPLS TE tunnels in the OSPFv3 router link-state advertisement (LSA) in the same way that other links appear for purposes of routing and forwarding traffic. The user can assign an OSPFv3 cost to the tunnel to give it precedence over other links. Other networking devices will see the tunnel as a link in addition to the physical link.

OSPFv3 uses Autoroute Announce (AA) or Forwarding Adjacencies (FA) feature to install IPv6 routes over MPLS/TE IPv4 tunnels into the IPv6 routing table . The TE tunnels are created using IPv4, and requires the use of a routing protocol other than OSPFv3. OSPFv2 is used as the IPv4 IGP and provides data which TE uses to create the tunnels.

OSPFv3 is configured on the TE tunnel interfaces for either autoroute-annouce or forwarding-adjacency. It is also must be configured in router mode to advertise the address of the loopback interface which TE is using for the tunnels that terminate on the router. That address is advertised in the TE LSA .

How to Configure Autoroute Announce and Forwarding Adjacencies For OSPFv3

Configuring Autoroute Announce and Forwarding Adjacencies For OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **interface** *type number*
5. **ip address** *ip-address-mask*
6. **no shutdown**
7. **exit**
8. **interface** *type number*
9. **ospfv3** *pid af* **mpls traffic-eng autoroute announce area** *aid*
10. **ospfv3** *pid af* **mpls traffic-eng autoroute metric** {*metric* | **absolute** *metric* | **relative** *delta*}
11. **ip ospf cost** *cost*
12. **exit**
13. **interface** *type number*
14. **ospfv3** *pid af* **mpls traffic-eng forwarding-adj area***aid*
15. **ospfv3**[*pid* [*af*]] **mpls traffic-eng forwarding-adj** *interface ID* [**local** *ID*] [**nbr** *ID*]
16. **ip ospf cost** *cost*
17. **exit**
18. **router ospfv3** *router-ID*
19. **address-family ipv4 unicast** [**vrf** *vrf-name*]
20. **area** *aid* **mpls traffic-engineering tunnel-tail** *af interface type*
21. **exit**
22. **show ospfv3 database**
23. **show ospfv3 mpls traffic-eng**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Device(config)# ip cef distributed`	Enables distributed Cisco Express Forwarding operation.
Step 4	**interface** *type number* **Example:** `Device(config)# interface tunnel 0`	Configures an interface type and enters interface configuration mode.
Step 5	**ip address** *ip-address-mask* **Example:** `Device (config-if)# ip address 192.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for the specified interface.
Step 6	**no shutdown** **Example:** `Device (config-if)# no shutdown`	Disables all functions on the specified interface.
Step 7	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 8	**interface** *type number* **Example:** `Device (config)# interface loopback 0`	Enables loopback interface and enters interface configuration mode.
Step 9	**ospfv3** *pid af* **mpls traffic-eng autoroute announce area** *aid* **Example:** `Device(config-if)# ospfv3 1 af mpls traffic-eng autoroute announce area 1`	Enable Open Shortest Path First version 3 (OSPFv3) on an interface with the IP address family (AF).
Step 10	**ospfv3** *pid af* **mpls traffic-eng autoroute metric** {*metric* | **absolute** *metric* | **relative** *delta*} **Example:** `Device(config-if)# ospfv3 1 af mpls traffic-eng autoroute metric 1`	Specifies the MPLS traffic engineering auto route metric value for the SPF calculation.

	Command or Action	Purpose
Step 11	**ip ospf cost** *cost* **Example:** `Device(config-if)# ip ospf cost 60`	Explicitly specifies the cost of sending a packet on an OSPF interface.
Step 12	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 13	**interface** *type number* **Example:** `Device (config)# interface tunnel 1`	Enables tunnel interface and enters interface configuration mode.
Step 14	**ospfv3** *pid af* **mpls traffic-eng forwarding-adj area***aid* **Example:** `Device(config-if)# ospfv3 1 af mpls traffic-eng forwarding-adj area 1`	Configure an MPLS traffic engineering forwarding adjacency.
Step 15	**ospfv3**[*pid* [*af*]] **mpls traffic-eng forwarding-adj** *interface ID* [**local** *ID*] [**nbr** *ID*] **Example:** `Device(config-if)# ospfv3 1 af mpls traffic-eng forwarding-adj 1`	Specifies the MPLS traffic engineering forwarding adjacency for the SPF calculation.
Step 16	**ip ospf cost** *cost* **Example:** `Device(config-if)# ip ospf cost 55`	Explicitly specifies the cost of sending a packet on an OSPF interface.
Step 17	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 18	**router ospfv3** *router-ID* **Example:** `Device(config)# router ospfv3 18`	Enters OSPFv3 router configuration mode.
Step 19	**address-family ipv4 unicast** [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv4 unicast`	Configures the IPv4 address family in the OSPFv3 process and enters IPv4 address family configuration mode.

	Command or Action	Purpose
Step 20	**area** *aid* **mpls traffic-engineering tunnel-tail** *af interface type* **Example:** `Device(config-router-af)# area 1 mpls traffic-engineering tunnel-tail af loopback`	Configures OSPFv3 on the tail end of the traffic engineering tunnels.
Step 21	**exit** **Example:** `Device(config-router-af)# exit`	Exits address family configuration mode and returns to global configuration mode.
Step 22	**show ospfv3 database** **Example:** `Device(config)# show ospfv3 database`	(Optional) Displays list of information related to the OSPFv3 database for a specific router.
Step 23	**show ospfv3 mpls traffic-eng** **Example:** `Device(config)# show ospfv3 mpls traffic-eng`	(Optional) Displays autoroute announce, forwarding adjacency, and tunnel-tail information related to OSPFv3.

Configuration Examples for Autoroute Announce and Forwarding Adjacencies For OSPFv3

Example: Configuring Autoroute Announce and Forwarding Adjacencies For OSPFv3

```
!
ip cef distributed
interface tunnel 0
 ip address 192.108.1.27 255.255.255.0
 no shutdown

interface loopback 0
 ospfv3 1 af mpls traffic-eng autoroute announce area 1
 ospfv3 1 af mpls traffic-eng autoroute metric 1
 ip ospf cost 60

interface tunnel 1
 ospfv3 1 af mpls traffic-eng forwarding-adj area 1
 ospfv3 1 af mpls traffic-eng forwarding-adj nbr 1
 ip ospf cost 55

router ospfv3 18
 address-family ipv4 unicast
```

```
   area 1 mpls traffic-engineering tunnel-tail af loopback

  !
 !
!
```

Additional References for Autoroute Announce and Forwarding Adjacencies For OSPFv3

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF features	IP Routing: OSPF Configuration Guide

Standards and RFCs

Related Topic	Document Title
Advertising a Router's Local Addresses in OSPF Traffic Engineering (TE) Extensions	RFC5786
Traffic Engineering Extensions to OSPF Version 3	RFC5329
Traffic Engineering (TE) Extensions to OSPF Version 2	RFC3630

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

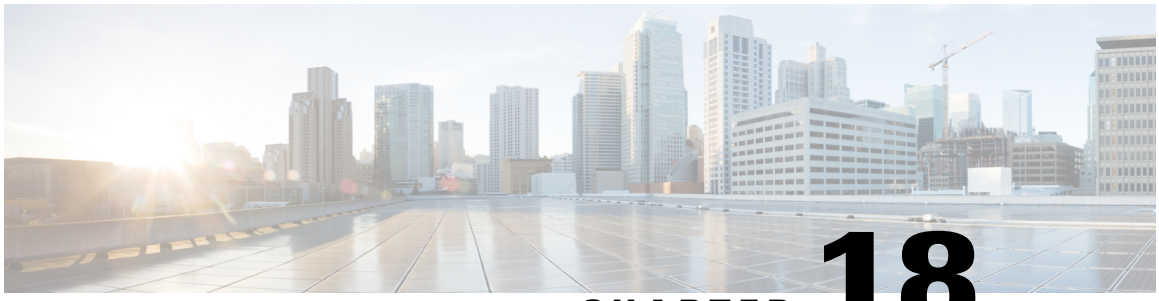
Feature Information for Autoroute Announce and Forwarding Adjacencies For OSPFv3

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 20: Feature Information for Autoroute Announce and Forwarding Adjacencies For OSPFv3

Feature Name	Releases	Feature Information
Autoroute Announce and Forwarding Adjacencies For OSPFv3	Cisco IOS XE Release 3.12S	The Autoroute Announce and Forwarding Adjacencies For OSPFv3 feature advertises IPv6 routes over MPLS/TE IPv4 tunnels. The following commands were introduced or modified: **ospfv3 af mpls traffic-eng autoroute announce area** , **ospfv3 mpls traffic-eng autoroute metric**, **ospfv3 mpls traffic-eng forwarding-adj area** .



CHAPTER 18

OSPFv3 Autoroute Exclude

OSPFv3 Autoroute Exclude feature allows you to use specific destinations and prefix-list to specify a list of prefixes that are routed using native paths instead of TE tunnels for packet transport. The rest of the prefixes can still be set to use TE tunnels. Prefixes that are excluded do not use a TE tunnel path. IPv6 routes over TE tunnels are supported by OSPFv3 using Autoroute Announce (AA) or Forwarding Adjacencies (FA).

This module describes how to configure the OSPFv3 Autoroute Exclude feature.

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.

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 OSPFv3 Autoroute Exclude

- Open Shortest Path First (OSPF) must be configured in your network.
- Cisco Express Forwarding (CEF) must be enabled.

- Multiprotocol Label Switching (MPLS) TE tunnels must be configured.
- Auto route announce and forwarding adjacencies must be configured. You can configure either auto route announce or forwarding adjacencies on an interface. You cannot configure them both on the same interface.

Information About OSPFv3 Autoroute Exclude

Overview of OSPFv3 Autoroute Exclude

The auto route feature is an IP routing method that forces OSPF to use MPLS TE tunnels to build paths for IP traffic routes. The auto route feature enables all routes to use TE Tunnels, even if there is an alternate non-TE path available for that route.

The OSPFv3 Autoroute Exclude feature allows specific IPv6 destinations or prefixes to avoid TE tunnels, while other prefixes can still be configured to use TE tunnels. Prefixes that are excluded do not use a TE tunnel path. Only native non-TE paths are downloaded to RIB for such routes. IPv6 routes over TE tunnels are supported by OSPFv3 using auto route announce (AA) or forwarding adjacencies (FA).

The auto route exclude option is configured under the router OSPF configuration mode by using a prefix list. IP addresses and prefixes that are members of this prefix list are excluded from TE tunnels, even when the auto route is enabled on them. If the IP addresses or prefixes are added to the prefix list, they are dynamically routed without passing through the TE tunnel. If the IP addresses or prefixes are removed from the prefix list, they are dynamically rerouted back on the TE tunnel path.

See the Autoroute Announce and Forwarding Adjacencies For OSPFv3 module in *IP Routing: OSPF Configuration Guide* for details on configuring auto route announce and forwarding adjacencies For OSPFv3.

How to Configure OSPFv3 Autoroute Exclude

Configuring OSPFv3 Autoroute Exclude

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-ID*
4. **address-family ipv6 unicast**
5. **mpls traffic-engineering autoroute-exclude prefix-list** *prefix-list-name*
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 18`	Configures OSPFv3 routing process and enters OSPF router configuration mode.
Step 4	**address-family ipv6 unicast** **Example:** `Device(config-router)# address-family ipv6 unicast`	Enters IPv6 address family configuration mode for OSPFv3.
Step 5	**mpls traffic-engineering autoroute-exclude prefix-list** *prefix-list-name* **Example:** `Device(config-router-af)# mpls traffic-engineering autoroute-exclude prefix-list kmd`	Allows specific destinations and prefixes to avoid routing through TE tunnels. • Prefixes that are excluded do not use a TE tunnel path.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv3 Autoroute Exclude

Example: Configuring OSPFv3 Autoroute Exclude

```
!
router ospfv3 18
 address-family ipv6 unicast
  mpls traffic-engineering autoroute-exclude prefix-list kmd

!
```

Additional References for OSPFv3 Autoroute Exclude

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF	*IP Routing: OSPF Configuration Guide*
Autoroute Announce and Forwarding Adjacencies For OSPFv3	*IP Routing: OSPF Configuration Guide*
Configuring Basic Cisco Express Forwarding	*IP Switching: Cisco Express Forwarding Configuration Guide*
MPLS Traffic Engineering Tunnel Source	*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

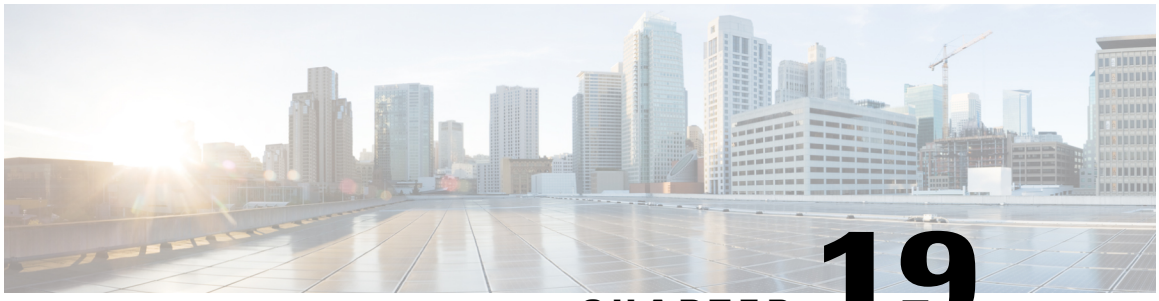
Feature Information for OSPFv3 Autoroute Exclude

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 21: Feature Information for OSPFv3 Autoroute Exclude

Feature Name	Releases	Feature Information
OSPFv3 Autoroute Exclude	Cisco IOS XE 3.14S	OSPFv3 Autoroute Exclude feature allows you to use specific destinations and prefix-list to specify a list of prefixes that are routed using native paths instead of TE tunnels for packet transport. IPv6 routes over TE tunnels are supported by OSPFv3 using autoroute announce or forwarding adjacencies. The following commands were introduced or modified: **mpls traffic-engineering autoroute-exclude prefix list**.



CHAPTER 19

OSPFv2 IP FRR Local Microloop Avoidance

The OSPFv2 IP FRR Local Microloop Avoidance feature helps to avoid local microloop that happens between a node and its neighbor where the link-down event occurred. This document explains how to configure the OSPFv2 IP FRR Local Microloop Avoidance feature.

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.

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 OSPFv2 IP FRR Local Microloop Avoidance

Overview of OSPFv2 IP FRR Local Microloop Avoidance

IP fast reroute (IPFRR) provides rapid convergence during the link-down events by moving the traffic to a pre computed backup path until the regular convergence mechanisms move the traffic to the newly found best path referred to as the post-convergence path.

Once the traffic is moved to the post-convergence path, it is inclined to a microloop. Microloops are formed as a result of the fact that each node on the path does its calculation at different times and independently of other nodes. If certain nodes converge and sends traffic to a neighbor node, which has not converged yet, traffic may be looped between these two nodes.

Microloops are formed between the router where the failure is detected and its neighbors. Local microloops are created in cases where there is no local loop-free alternate (LFA) backup available in ring or square topologies. In such topologies, remote LFA provides a backup, but the fast-convergence benefit of the remote LFA cannot be completely utilized due to the high probability of the local microloop creation. Avoiding the local micro loop provides a significant improvement in the fast convergence in the ring and square topologies.

Note Microloop avoidance is automatically enabled as soon as remote LFA (rLFA) is enabled.

When using microloop avoidance for prefixes (for which a repair path has been installed in the forwarding plane), the OSPFv2 IP FRR Local Microloop Avoidance feature is enabled when the forwarding plane is triggered to switch to using a pre installed repair path. The local microloop avoidance for the link-down event supports the following triggers:

- Interface down event.
- Adjacency down event due to the Bidirectional Forwarding Detection (BFD) session down.

If microloop avoidance is used regardless of whether a repair path has been installed in the forwarding plane, then in addition the third trigger is used:

- Adjacency down event due to neighbor hold time expiration.

When the neighbor reports loss of adjacency to the local system in its link state neighbor advertisements, the value of using microloop avoidance depends on whether the remote event that caused loss of adjacency on the neighbor is detectable by the local forwarding plane (that is, whether the forwarding plane will react and switch to using pre programmed repair paths).

How to Configure OSPFv2 IP FRR Local Microloop Avoidance

Configuring OSPFv2 IP FRR Local Microloop Avoidance

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **microloop avoidance** [**protected** | **disable**]
5. **microloop avoidance rib-update-delay** *delay-period*
6. **exit**

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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Configures an OSPF routing process and enters router configuration mode.
Step 4	**microloop avoidance** [**protected** | **disable**] **Example:** `Device(config-router)# microloop avoidance protected`	Configures the local microloop avoidance between a node and its neighbor where the link-down event has occurred. • When the **protected** keyword is used, the local microloop avoidance is only applied to prefixes that have a valid backup path. • When the **disable** keyword is used, the local microloop avoidance is disabled if it is enabled automatically earlier.
Step 5	**microloop avoidance rib-update-delay** *delay-period* **Example:** `Device(config-router)# microloop avoidance rib-update-delay 6500`	Delays the local microloop avoidance as per the configured delay period.
Step 6	**exit** **Example:** `Device(config-router)# exit`	Exits router configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv2 IP FRR Local Microloop Avoidance

Example: Configuring OSPFv2 IP FRR Local Microloop Avoidance

```
router ospf 10
 microloop avoidance protected
```

```
microloop avoidance rib-update-delay 6500
!
```

Additional References for OSPFv2 IP FRR Local Microloop Avoidance

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF features	IP Routing: OSPF Configuration Guide

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

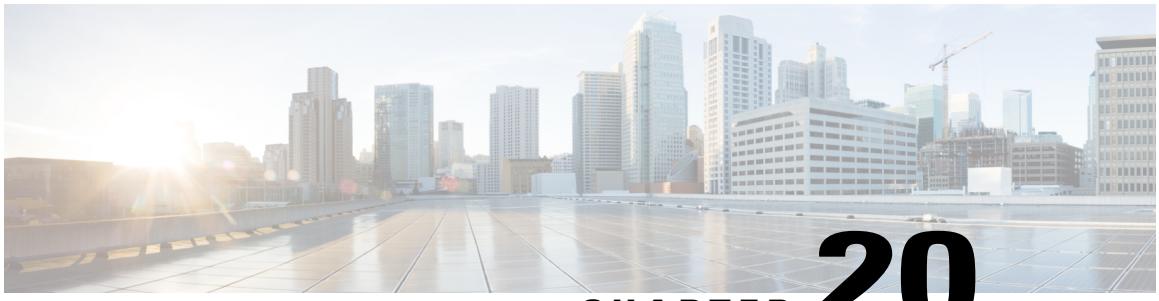
Feature Information for OSPFv2 IP FRR Local Microloop Avoidance

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 22: Feature Information for OSPFv2 IP FRR Local Microloop Avoidance

Feature Name	Releases	Feature Information
OSPFv2 IP FRR Local Microloop Avoidance	Cisco IOS XE Release 3.11S 15.4(1)S	The OSPFv2 IP FRR Local Microloop Avoidance feature helps to avoid local microloop that happens between a node and its neighbor where the link-down event occurred. The following commands were introduced or modified: **microloop avoidance**, **microloop avoidance rib-update-delay**.



CHAPTER 20

OSPFv2-OSPF Live-Live

The OSPFv2-OSPF Live-Live feature delivers multicast streams over non overlapping paths to various applications. The multicast traffic is split into multiple streams at the beginning of a protected network. All streams flow over non overlapping paths so that when a link failure occurs on one path, multicast traffic is still delivered through other paths. All streams are merged back at the end of the protected network. This module describes how to configure the OSPFv2-OSPF Live-Live feature.

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.

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 OSPFv2-OSPF Live-Live

Overview of OSPFv2-OSPF Live-Live

Many new applications driving the growth of networking market are multicast based. Applications such as Internet Protocol television (IPTV) are typically associated with simultaneously delivering massive amount

of sensitive data streams to large audiences. Packet drop is a critical issue in multimedia traffic. There is a demand to reduce multicast traffic loss to the range of milliseconds or to zero packet loss. The zero packet loss solution for multicast in case of single link failure is also known as live-live.

In a live-live network, multicast streams (typically two flows) form their own reverse path forwarding (RPF)/shortest path trees (SPT) over diversified physical links, so that failure on one link does not affect multicast traffic on other link. The existing multi topology technology in Cisco IOS software supports the multiple multicast topologies.

The OSPFv2-OSPF Live-Live feature enables the protocol independent multicast (PIM) to handle multiple multicast topologies. When a multicast topology is created and enabled on OSPF, IP prefixes on each topology are injected into topology-based Routing Information Base (RIB). PIM then decides which RIB to use for RPF lookup.

PIM RPF topology is a collection of routes used by PIM to perform the RPF operation when building shared or source trees. In a multi topology environment, multiple RPF topologies can be created in the same network. A particular source may be reachable in only one of the topologies or in several of them through different paths.

To select the RPF topology for a particular multicast distribution tree, consider the following:

1. Configure a policy that maps a group range to a topology. When RPF information needs to be resolved for the RP or the sources for a group within the range, the RPF lookup takes place in the specified topology. This can be used for PIM Sparse Mode (PIM-SM)/source-specific multicast (SSM)/Bidirectional(Bidir) PIM.
2. Configure a policy that maps a source prefix range to a topology. This can be used for PIM-SM and PIM-SSM.
3. Use the topology identified by the Join Attribute encoding in the received PIM packets.

The PIM Join Attribute extends PIM signaling to identify a topology that should be used when constructing a particular multicast distribution tree. For more details on the PIM Join Attribute, see PIM Multi-Topology ID (MT-ID) Join-Attribute IEEE draft.

How to Configure OSPFv2-OSPF Live-Live

Configuring OSPFv2-OSPF Live-Live

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **ip multicast rpf multitopology**
5. **global-address-family ipv4 multicast**
6. **topology** {*topology-A* | *topology-B*}
7. **exit**
8. **interface** *type number*
9. **ip address** *address mask*
10. **ip pim sparse-dense-mode**
11. **ip ospf** *process-id* **area** *area-id*
12. **topology ipv4 multicast** *topology-name*
13. **exit**
14. **router ospf** *process-id*
15. **network** *ip-adddress mask* **area** *area-id*
16. **address-family ipv4 multicast**
17. **topology** *topology-name* **tid** *topology-id*
18. **end**
19. **configure terminal**
20. **ip multicast topology multicast** *topology-name* **tid** *topology-id*
21. **ip multicast rpf select topology multicast** *topology-name access-list number*
22. **ip access-list extended** *access-list-number*
23. **permit ip any** *ip-adddress*
24. **end**
25. **show ip multicast topology multicast** *topology-name*
26. **debug ip multicast topology**

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	**ip multicast-routing** **Example:** `Device(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**ip multicast rpf multitopology** **Example:** `Device(config)# ip multicast rpf multitopology`	Enables Multi Topology Routing (MTR) support for IP multicast routing.
Step 5	**global-address-family ipv4 multicast** **Example:** `Device(config)# global-address-family ipv4 multicast`	Enters global address family configuration mode and configures multi topology routing.
Step 6	**topology** {*topology-A* | *topology-B*} **Example:** `Device(config-af)# topology live-A`	Configures an OSPF process to route IP traffic under the specified topology instance.
Step 7	**exit** **Example:** `Device(config-af)# exit`	Exits address family configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface Gigabitethernet 1/0`	Configures an interface type and enters interface configuration mode.
Step 9	**ip address** *address mask* **Example:** `Device(config-if)# ip address 192.108.1.27 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 10	**ip pim sparse-dense-mode** **Example:** `Device(config-if)# ip pim sparse-dense-mode`	Enables PIM on an interface and treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.

	Command or Action	Purpose
Step 11	**ip ospf** *process-id* **area** *area-id* **Example:** `Device(config-if)# ip ospf 10 area 0`	Enables OSPFv2 on an interface.
Step 12	**topology ipv4 multicast** *topology-name* **Example:** `Device(config-if)# topology ipv4 multicast live-A`	Configures a multi topology instance on an interface.
Step 13	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and enters global configuration mode. • Repeat Steps 9 to 12 to configure the next topology (**topology ipv4 multicast live-B**).
Step 14	**router ospf** *process-id* **Example:** `Device(config)# router ospf 102`	Enables OSPF routing and enters router configuration mode.
Step 15	**network** *ip-adddress mask* **area** *area-id* **Example:** `Device(config-router)# network 192.168.129.16 0.0.0.3 area 20`	Defines an interface on which OSPF runs and defines the area ID for that interface.
Step 16	**address-family ipv4 multicast** **Example:** `Device(config-router)# address-family ipv4 multicast`	Enters router address family configuration mode and configures OSPF to exchange IPv4 multicast prefixes.
Step 17	**topology** *topology-name* **tid** *topology-id* **Example:** `Device(config-router-af)# topology live-A tid 100`	Configures an OSPF process to route IP traffic under the specified topology instance. • Repeat this step to configure the OSPF process to route IP traffic under another topology instance (**topology live-B tid 200**).
Step 18	**end** **Example:** `Device(config-router-af)# end`	Exits router address family configuration mode and returns to privileged EXEC mode.
Step 19	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 20	**ip multicast topology multicast** *topology-name* **tid** *topology-id*	Configures topology selection for the multicast streams.

	Command or Action	Purpose
	Example: `Device(config)# ip multicast topology multicast live-A tid 100`	• Repeat this step to configure another topology (**ip multicast topology multicast live-B tid 200**).
Step 21	**ip multicast rpf select topology multicast** *topology-name access-list number* **Example:** `Device(config)# ip multicast rpf select topology multicast topology live-A 111`	Associates a multicast topology with a multicast group with a specific route entry. • Repeat this step to associate the topology with another multicast group (**ip multicast rpf select topology multicast live-B 122**).
Step 22	**ip access-list extended** *access-list-number* **Example:** `Device(config)# ip access-list extended 111`	Defines an IP access list to enable filtering for packets with IP helper-address destinations and enters extended named access list configuration mode.
Step 23	**permit ip any** *ip-adddress* **Example:** `Device(config-ext-nacl)# permit ip any 203.0.113.1`	Sets condition to allow a packet to pass a named IP access list. • Repeat Steps 22 and 23 to define another IP access list and to set conditions to allow a packet to pass another named IP access list.
Step 24	**end** **Example:** `Device(config-ext-nacl)# end`	Exits extended named access list configuration mode and enters privileged EXEC mode.
Step 25	**show ip multicast topology multicast** *topology-name* **Example:** `Device# show ip multicast topology multicast live-A`	Displays topology information for multicast streams.
Step 26	**debug ip multicast topology** **Example:** `Device# debug ip multicast topology`	Enables debugging output for multicast stream topology.

Configuration Examples for OSPFv2-OSPF Live-Live

Example: Configuring OSPFv2-OSPF Live-Live

```
ip multicast-routing
!
ip multicast rpf multitopology
```

```
!
global-address-family ipv4 multicast
  topology live-A
  topology live-B

int gigabitethernet 1/0
 ip address 192.0.2.1 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf 10 area 20
 topology ipv4 multicast live-A
!
int gigabitethernet 2/0
 ip address 192.0.2.2 255.255.255.0
 ip pim sparse-dense-mode
 ip ospf 11 area 21
 topology ipv4 multicast live-B
!
router ospf 1
 network 192.168.129.16 0.0.0.3 area 20
  address-family ipv4 multicast
  !!
   topology live-A tid 10
   topology live-B tid 20
!
!!
ip multicast topology multicast live-A tid 100
ip multicast topology multicast live-B tid 200
!
!!
ip multicast rpf select topology multicast live-A 111
ip multicast rpf select topology multicast live-B 122

!
 ip access-list extended 111
 permit ip any 203.0.113.254

ip access-list extended 122
 permit ip any 203.0.113.251
```

Additional References for OSPFv2-OSPF Live-Live

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Configuring OSPF features	IP Routing: OSPF Configuration Guide

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

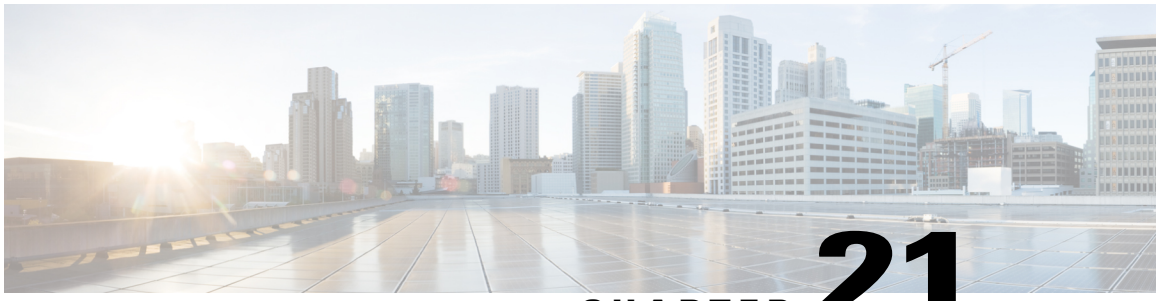
Feature Information for OSPFv2-OSPF Live-Live

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 23: Feature Information for OSPFv2-OSPF Live-Live

Feature Name	Releases	Feature Information
OSPFv2-OSPF Live-Live	Cisco IOS XE Release 3.11S	The OSPFv2-OSPF Live-Live feature delivers multicast streams over non overlapping paths to various applications. The multicast traffic is split into multiple streams at the beginning of a protected network. All streams flow over non overlapping paths so that when a link failure occurs on one path, multicast traffic is still delivered through other paths. All streams are merged back at the end of the protected network. No commands were introduced or modified.



CHAPTER 21

OSPF Forwarding Address Suppression in Translated Type-5 LSAs

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes a not-so-stubby area (NSSA) area border router (ABR) to translate Type-7 link state advertisements (LSAs) to Type-5 LSAs, but to use the address 0.0.0.0 for the forwarding address instead of that specified in the Type-7 LSA. This feature causes devices that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ABRs.

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.

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 Forwarding Address Suppression

This document presumes that you have OSPF configured on the networking device; it does not document other steps to configure OSPF.

Information About OSPF Forwarding Address Suppression

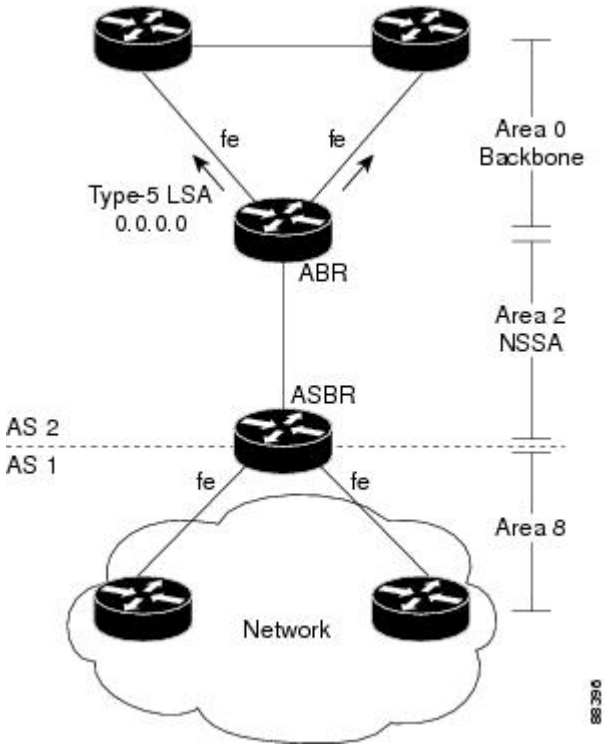
Benefits of OSPF Forwarding Address Suppression

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes an NSSA ABR to translate Type-7 LSAs to Type-5 LSAs, but use the 0.0.0.0 as the forwarding address instead of that specified in the Type-7 LSA. This feature causes devices that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ASBRs.

When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs

In the figure below, it would be advantageous to filter Area 2 addresses from Area 0 to minimize the number of routes introduced into the backbone (Area 0). However, using the **area range**command to consolidate and summarize routes at the area boundary--filtering the Area 2 addresses--will not work because the Area 2 addresses include forwarding addresses for Type-7 LSAs that are generated by the ASBR. If these Type-7 LSA forwarding addresses have been filtered out of Area 0, the backbone routers cannot reach the prefixes advertised in the translated Type-5 LSAs (autonomous system external LSAs).

Figure 9: OSPF Forwarding Address Suppression in Translated Type-5 LSAs



This problem is solved by suppressing the forwarding address on the ABR so that the forwarding address is set to 0.0.0.0 in the Type-5 LSAs that were translated from Type-7 LSAs. A forwarding address set to 0.0.0.0

indicates that packets for the external destination should be forwarded to the advertising OSPF device, in this case, the translating NSSA ABR.

Before configuring this feature, consider the following caution.

Caution Configuring this feature causes the device to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

How to Suppress the OSPF Forwarding Address

Suppressing the OSPF Forwarding Address in Translated Type-5 LSAs

This task describes how to suppress the OSPF forwarding address in translated Type-5 LSAs. Before configuring this feature, consider the following caution.

Caution Configuring this feature causes the device to be noncompliant with RFC 1587. Also, suboptimal routing might result because there might be better paths to reach the destination's forwarding address. This feature should not be configured without careful consideration and not until the network topology is understood.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **area** *area-id* **nssa translate type7 suppress-fa**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables higher privilege levels, such as 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 ospf** *process-id* **Example:** `Device(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**area** *area-id* **nssa translate type7 suppress-fa** **Example:** `Device(config-router)# area 10 nssa translate type7 suppress-fa`	Configures an area as a not-so-stubby-area (NSSA) and suppresses the forwarding address in translated Type-7 LSAs.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPF Forwarding Address Suppression

Suppressing OSPF Forwarding Address in Translated Type-5 LSAs Example

This example suppresses the forwarding address in translated Type-5 LSAs:

```
interface gigabitethernet 0/0/0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface gigabitethernet 0/01
 ip address 10.94.1.1 255.255.255.0
!
router ospf 1
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 network 10.94.0.0 0.0.255.255 area 10
 area 10 nssa translate type7 suppress-fa
```

Additional References

The following sections provide references related to OSPF Forwarding Address Suppression in Translated Type-5 LSAs:

Related Documents

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF"
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases
OSPFv3 Address Families	" *OSPFv3 Address Families*" module

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 releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1587	*The OSPF NSSA Option* **Note** Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587, *The OSPF NSSA Option* .

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

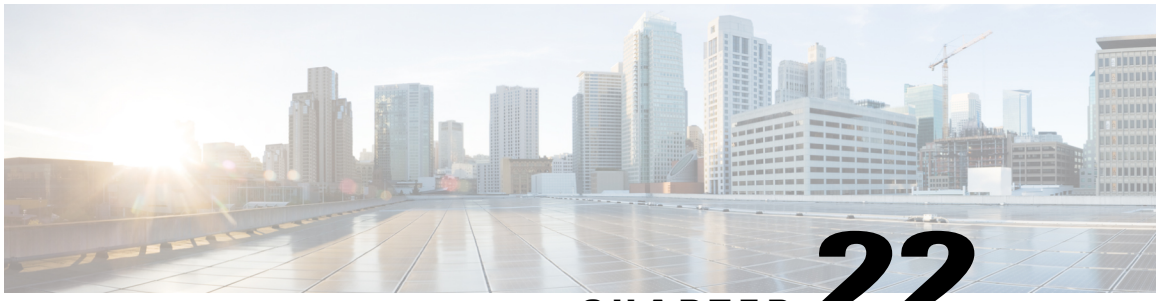
Feature Information for OSPF Forwarding Address Suppression

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 24: Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

Feature Name	Releases	Feature Information
OSPF Forwarding Address Suppression in Translated Type-5 LSAs	Cisco IOS XE Release 2.1	The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes a not-so-stubby area (NSSA) area border router (ABR) to translate Type-7 link state advertisements (LSAs) to Type-5 LSAs, but to use the address 0.0.0.0 for the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ABRs. The following commands are introduced or modified in the feature documented in this module: • **area nssa translate** • **show ip ospf**



CHAPTER 22

OSPF Inbound Filtering Using Route Maps with a Distribute List

The OSPF Inbound Filtering Using Route Maps with a Distribute List feature allows users to define a route map to prevent Open Shortest Path First (OSPF) routes from being added to the routing table. In the route map, the user can match on any attribute of the OSPF route.

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.

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 OSPF Inbound Filtering Using Route Maps with a Distribute List

It is presumed that you have OSPF configured in your network.

Information About OSPF Inbound Filtering Using Route Maps with a Distribute List

Benefits of OSPF Route-Map-Based-Filtering

Users can define a route map to prevent OSPF routes from being added to the routing table. This filtering happens at the moment when OSPF is installing the route in the routing table. This feature has no effect on LSA flooding. In the route map, the user can match on any attribute of the OSPF route. That is, the route map could be based on the following **match** options:

- **match interface**
- **match ip address**
- **match ip next-hop**
- **match ip route-source**
- **match metric**
- **match route-type**
- **match tag**

This feature can be useful during redistribution if the user tags prefixes when they get redistributed on ASBRs and later uses the tag to filter the prefixes from being installed in the routing table on other routers.

Filtering Based on Route Tag

Users can assign tags to external routes when they are redistributed to OSPF. Then the user can deny or permit those routes in the OSPF domain by identifying that tag in the **route-map** and **distribute-list in** commands.

Filtering Based on Route Type

In OSPF, the external routes could be Type 1 or Type 2. Users can create route maps to match either Type 1 or Type 2 and then use the **distribute-list in** command to filter certain prefixes. Also, route maps can identify internal routes (interarea and intra-area) and then those routes can be filtered.

Filtering Based on Route Source

When a match is done on the route source, the route source represents the OSPF Router ID of the LSA originator of the LSA in which the prefix is advertised.

Filtering Based on Interface

When a match is done on the interface, the interface represents the outgoing interface for the route that OSPF is trying to install in the routing table.

Filtering Based on Next-Hop

When a match is done on the next hop, the next hop represents the next hop for the route that OSPF is trying to install in the routing table.

How to Configure OSPF Inbound Filtering Using Route Maps

Configuring OSPF Inbound Filtering Using a Route Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [**permit** | **deny**] [*sequence-number*]
4. **match tag** *tag-name*
5. Repeat Steps 3 and 4 with other **route-map** and **match** commands if you choose.
6. **exit**
7. **router ospf** *process-id*
8. **distribute-list route-map** *map-tag* **in**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Router(config)# route-map tag-filter deny 10`	Defines a route map to control filtering.
Step 4	**match tag** *tag-name* **Example:** **Example:** `or other` **match** `commands`	Matches routes with a specified name, to be used as the route map is referenced. • At least one **match** command is required, but it need not be this **match**command. This is just an example. • The list of **match** commands available to be used in this type of route map appears on the **distribute-list in** command reference page.

	Command or Action	Purpose
	Example: `Router(config-router)# match tag 777`	• This type of route map will have no **set** commands.
Step 5	Repeat Steps 3 and 4 with other **route-map** and **match** commands if you choose.	--
Step 6	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode.
Step 7	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 8	**distribute-list route-map** *map-tag* **in** **Example:** `Router(config-router)# distribute-list route-map tag-filter in`	Enables filtering based on an OSPF route map.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Inbound Filtering Using Route Maps with a Distribute List

Example OSPF Route-Map-Based Filtering

In this example, OSPF external LSAs have a tag. The value of the tag is examined before the prefix is installed in the routing table. All OSPF external prefixes that have the tag value of 777 are filtered (prevented from being installed in the routing table). The permit statement with sequence number 20 has no match conditions, and there are no other route-map statements after sequence number 20, so all other conditions are permitted.

```
route-map tag-filter deny 10
 match tag 777
route-map tag-filter permit 20
```

```
!
router ospf 1
 router-id 10.0.0.2
 log-adjacency-changes
 network 172.16.2.1 0.0.0.255 area 0
 distribute-list route-map tag-filter in
```

Additional References

The following sections provide references related to configuring the OSPF Inbound Filtering Using Route Maps with a Distribute List feature.

Related Documents

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF"
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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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

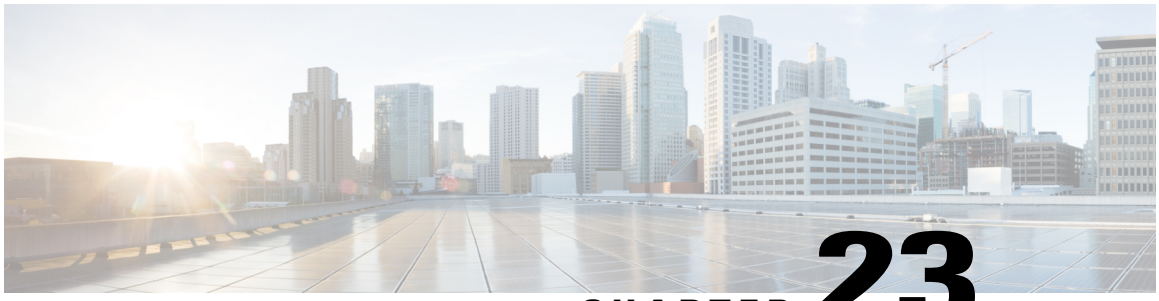
Feature Information for OSPF Inbound Filtering Using Route Maps with a Distribute List

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 25: Feature Information for OSPF Inbound Filtering Using Route Maps with a Distribute List

Feature Name	Releases	Feature Information
OSPF Inbound Filtering Using Route Maps with a Distribute List	Cisco IOS XE Release 2.1	The OSPF Inbound Filtering Using Route Maps with a Distribute List feature allows users to define a route map to prevent OSPF routes from being added to the routing table. The following commands are introduced or modified in the feature documented in this module: • **distribute-list in (IP)**



CHAPTER 23

OSPFv3 Route Filtering Using Distribute-List

The OSPFv3 route filtering using distribute-list feature allows users to filter the incoming routes that are programmed in routing table, and the outgoing routes that are advertised.

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 OSPFv3 Route Filtering Using Distribute-List

It is presumed that you have OSPF configured in your network.

Information About OSPFv3 Route Filtering Using Distribute-List

Users can define a route map to prevent OSPF routes from being added to the routing table. This filtering happens at the moment when OSPF is installing the route in the routing table. This feature has no effect on link-state advertisement (LSA) flooding.

This feature can be useful during redistribution if the user tags prefixes when they get redistributed on Autonomous System Boundary Routers (ASBRs) and later uses the tag to filter the prefixes from being installed in the routing table on other routers. The below mentioned options are available only for distribute-list filtering using route-map.

Filtering Based on Route Tag

Users can assign tags to external routes when they are redistributed to OSPF. Then the user can deny or permit those routes in the OSPF domain by identifying that tag in the **route-map** and **distribute-list in** or **distribute-list out** commands.

Filtering Based on Route Type

In OSPF, the external routes could be Type 1 or Type 2. Users can create route maps to match either Type 1 or Type 2 and then use the **distribute-list in** command to filter certain prefixes. Also, route maps can identify internal routes (interarea and intra-area) and then those routes can be filtered.

Filtering Based on Route Source

When a match is done on the route source, the route source represents the OSPF Router ID of the LSA originator of the LSA in which the prefix is advertised.

Filtering Based on Interface

When a match is done on the interface, the interface represents the outgoing interface for the route that OSPF is trying to install in the routing table.

Filtering Based on Next Hop

When a match is done on the next hop, the next hop represents the next hop for the route that OSPF is trying to install in the routing table.

Note The **distribute-list in** command can be configured to prevent routes from being installed in the global Routing Information Base (RIB). Prior to the implementation of OSPF local RIB (for feature information on OSPF local RIB, see OSPFv2 Local RIB), OSPF would attempt to install a less preferred route (e.g. an inter-area route when the intra-area path is filtered). With OSPF local RIB, only the best route is considered (because this is the only route the local RIB maintains). There is no concept of a "second-best" OSPF route. For more information on the routing algorithm used by Cisco OSPF routers, please refer to RFC 2328.

How to Configure OSPFv3 Route Filtering Using Distribute-List

Configuring OSPFv3 (IPv4 address-family)

Command Mode: Address family mode (address-family ipv4 unicast). Following is the syntax:

```
[no] distribute-list [<access-list #> | <access-list name>] |
                      {prefix <name1> gateway <name2>} |
                      {prefix <name1>} | {gateway <name2>} |
```

```
       {route-map name} in [<interface>]

[no] distribute-list [<access-list #> | <access-list name>] | [prefix <name>] out
      [{ <routing-process> | <interface> }]
```

Interface: Incoming (used with Inbound filtering) or outgoing (used with outbound filtering) interface.

Routing-process: Source protocol for the route to be filtered.

Configuring Inbound Filtering: Route Map

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv4 unicast.
3. Configure distribute list with the appropriate route-map.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv4 unicast.

```
Device(config-router)#address-family ipv4 unicast
```

Step 3 Configure distribute list with the appropriate route-map.

```
Device(config-router-af)#distribute-list route-map rmap-name in
```

The following match options in a route-map are supported:

- match interface
- match ip address
- match ip next-hop
- match ip route-source
- match metric
- match route-type
- match tag

Configuring Inbound Filtering: Prefix-List/Access-List

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv4 unicast.
3. Defines prefix list to be used and the direction for the filter.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv4 unicast.

```
Device(config-router)#address-family ipv4 unicast
```

Step 3 Defines prefix list to be used and the direction for the filter.

```
Device(config-router-af)#distribute-list prefix pfxname in
```

Note The following are the available optional arguments. You can use these arguments to filter based on incoming interface. Choose any interface that is available on your device.

```
Ethernet           IEEE 802.3
  Loopback           Loopback interface
  Null               Null interface
  Port-channel       Ethernet Channel of interfaces
  Serial             Serial
  Tunnel             Tunnel interface
  Vlan               Catalyst Vlans
```

Configuring Outbound Filtering

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv4 unicast.
3. Configure distribute list with the appropriate route-map.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv4 unicast.

```
Device(config-router)#address-family ipv4 unicast
```

Step 3 Configure distribute list with the appropriate route-map.

```
Device(config-router-af)#distribute-list prefix pfxlist-name out
```

Note The following are the available optional arguments. You can use these options to filter based on the source protocol of the route.

```
bgp         Border Gateway Protocol (BGP)
  connected  Connected
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis       ISO IS-IS
  lisp       Locator ID Separation Protocol (LISP)
  ospf       Open Shortest Path First (OSPF)
  ospfv3     OSPFv3
  rip        Routing Information Protocol (RIP)
  static     Static routes
```

Configuring Route Filtering Using Distribute-List for OSPFv3 (IPv6 address-family)

Mode: Address-family mode (address-family ipv6 unicast). Prefix-list and route-map are supported as filtering options. Following is the syntax:

```
[no] distribute-list prefix-list <name> in [<interface>]
[no] distribute-list route-map <name> in
[no] distribute-list prefix-list <name> out <routing-process>
```

Interface: Incoming (used with Inbound filtering) or outgoing (used with outbound filtering) interface.

Routing-process: Source protocol for the route to be filtered.

Configuring Inbound Filtering: Route Map

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv6unicast.
3. Define route map.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv6unicast.

```
Device(config-router)#address-family ipv6 unicast
```

Step 3 Define route map.

```
Device(config-router-af)#distribute-list route-map rmap-name in
```

The following match options in a route-map are supported:

- match interface
- match ip address
- match ip next-hop
- match metric
- match route-type
- match tag

Configuring Inbound Filtering: Prefix-List

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv6 unicast.
3. Define prefix list name.
4. Define filter incoming routing updates.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv6 unicast.

```
Device(config-router)#address-family ipv6 unicast
```

Step 3 Define prefix list name.

```
Device(config-router-af)#distribute-list prefix pfxlist-name
```

Step 4 Define filter incoming routing updates.

```
Device(config-router-af)#distribute-list prefix pfxname in
```

Note The following are the available optional arguments. You can use these arguments to filter based on incoming interface. Choose any interface that is available on your device.

```
Ethernet            IEEE 802.3
  Loopback            Loopback interface
  Null                Null interface
  Port-channel        Ethernet Channel of interfaces
  Serial              Serial
  Tunnel              Tunnel interface
  Vlan                Catalyst Vlans
```

Configuring Outbound Filtering

SUMMARY STEPS

1. Configure OSPFv3.
2. Configure address-family ipv6 unicast.
3. Define prefix list name.

DETAILED STEPS

Step 1 Configure OSPFv3.

```
Device(config)#router ospfv3 1
```

Step 2 Configure address-family ipv6 unicast.

```
Device(config-router)#address-family ipv6 unicast
```

Step 3 Define prefix list name.

```
Device(config-router-af)#distribute-list prefix-list pfxlist-name out
```

Note These are the available options for the routing process. The <**routing-process**> argument is mandatory for IPv6 outbound route filtering.

```
bgp         Border Gateway Protocol (BGP)
  connected  Connected Routes
  eigrp      Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis       ISO IS-IS
  lisp       Locator ID Separation Protocol (LISP)
  ospf       Open Shortest Path First (OSPFv3)
  rip        IPv6 Routing Information Protocol (RIPv6)
  static     Static Routes
```

Additional References

Related Documents

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

MIBs

MIBs	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

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

Technical Assistance

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

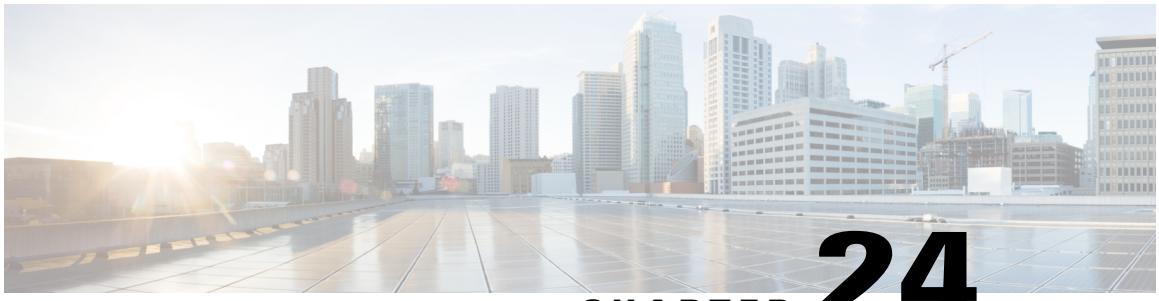
Feature Information for OSPFv3 Route Filtering Using Distribute-List

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 26: Feature Information for OSPFv3 Route Filtering Using Distribute-List

Feature Name	Releases	Feature Information
OSPFv3 Route Filtering Using Distribute-List	Cisco IOS XE Denali 16.3.1	The route-map support for OSPFv3 route-filtering using distribute-list is supported.



CHAPTER 24

OSPF Shortest Path First Throttling

The OSPF Shortest Path First Throttling feature makes it possible to configure shortest path first (SPF) scheduling in millisecond intervals and to potentially delay SPF calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology. One SPF run may include multiple topology change events.

The interval at which the SPF calculations occur is chosen dynamically and is based on the frequency of topology changes in the network. The chosen interval is within the boundary of the user-specified value ranges. If the network topology is unstable, SPF throttling calculates SPF scheduling intervals to be longer until the topology becomes stable.

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.

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 SPF Throttling

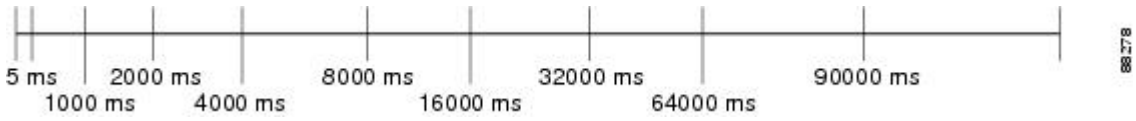
SPF calculations occur at the interval set by the **timers throttle spf**command. The wait interval indicates the amount of time to wait until the next SPF calculation occurs. Each wait interval after that calculation is twice as long as the previous one until the wait interval reaches the maximum wait time specified.

The SPF timing can be better explained using an example. In this example the start interval is set at 5 milliseconds (ms), the wait interval at 1000 milliseconds, and the maximum wait time is set at 90,000 milliseconds.

```
timers throttle spf 5 1000 90000
```

The figure below shows the intervals at which the SPF calculations occur so long as at least one topology change event is received in a given wait interval.

Figure 10: SPF Calculation Intervals Set by the timers throttle spf Command

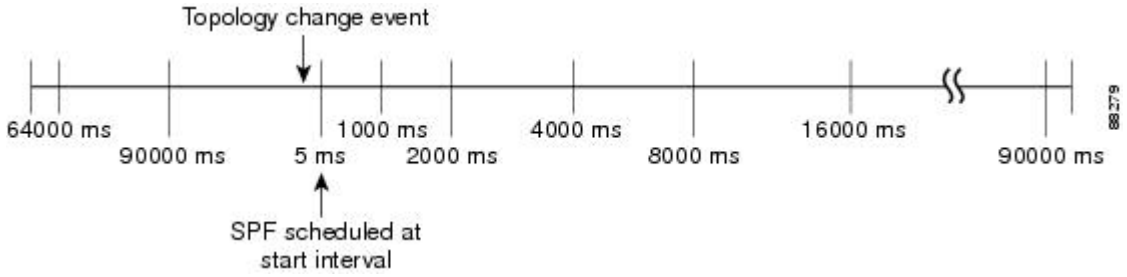


Notice that the wait interval between SPF calculations doubles when at least one topology change event is received during the previous wait interval. Once the maximum wait time is reached, the wait interval remains the same until the topology stabilizes and no event is received in that interval.

If the first topology change event is received after the current wait interval, the SPF calculation is delayed by the amount of time specified as the start interval. The subsequent wait intervals continue to follow the dynamic pattern.

If the first topology change event occurs after the maximum wait interval begins, the SPF calculation is again scheduled at the start interval and subsequent wait intervals are reset according the parameters specified in the **timers throttle spf**command. Notice in the figure below that a topology change event was received after the start of the maximum wait time interval and that the SPF intervals have been reset.

Figure 11: Timer Intervals Reset After a Topology Change Event



How to Configure OSPF SPF Throttling

Configuring OSPF SPF Throttling

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as 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* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **Example:** `Router(config-router)# timers throttle spf 10 4800 90000`	Sets OSPF throttling timers.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits configuration mode.

Verifying SPF Throttle Values

To verify SPF throttle timer values, use the **show ip ospf** command. The values are displayed in the lines that begin, "Initial SPF schedule delay...," "Minimum hold time between two consecutive SPFs...," and "Maximum wait time between two consecutive SPFs...."

```
Router# show ip ospf
 Routing Process "ospf 1" with ID 10.10.10.2 and Domain ID 0.0.0.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 It is an autonomous system boundary router
 Redistributing External Routes from,
    static, includes subnets in redistribution
Initial SPF schedule delay 5 msecs
 Minimum hold time between two consecutive SPFs 1000 msecs
 Maximum wait time between two consecutive SPFs 90000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 4. Checksum Sum 0x17445
 Number of opaque AS LSA 0. Checksum Sum 0x0
 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 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 19:11:15.140 ago
        SPF algorithm executed 28 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x2C1D4
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Configuration Example for OSPF SPF Throttling

Example Throttle Timers

This example shows a router configured with the start, hold, and maximum interval values for the **timers throttle spf** command set at 5, 1,000, and 90,000 milliseconds, respectively.

```
router ospf 1
 router-id 10.10.10.2
 log-adjacency-changes
 timers throttle spf 5 1000 90000
 redistribute static subnets
 network 21.21.21.0 0.0.0.255 area 0
 network 22.22.22.0 0.0.0.255 area 00
```

Additional References

The following sections provide references related to OSPF Shortest Path First Throttling.

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

Standards	Title
None	--

MIBs

MIBs	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

RFCs	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

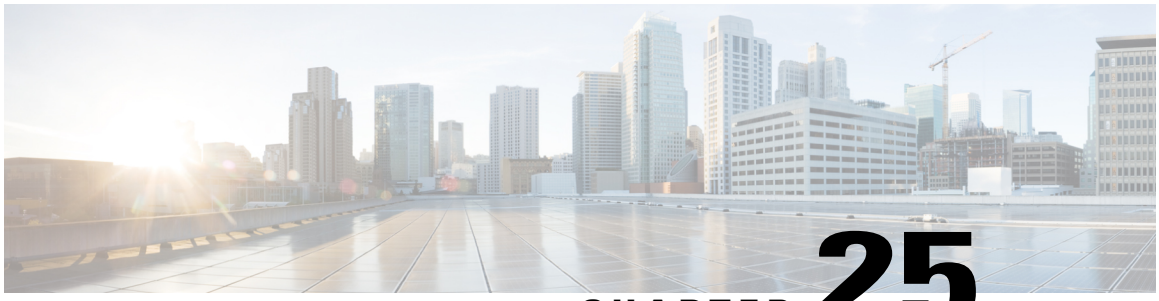
Feature Information for OSPF Shortest Path First Throttling

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 27: Feature Information for OSPF Shortest Path First Throttling

Feature Name	Releases	Feature Information
OSPF Shortest Path First Throttling	Cisco IOS XE Release 2.1	The OSPF Shortest Path First Throttling feature makes it possible to configure SPF scheduling in millisecond intervals and to potentially delay shortest path first (SPF) calculations during network instability. SPF is scheduled to calculate the Shortest Path Tree (SPT) when there is a change in topology. The following commands are introduced or modified in the feature documented in this module: • **timer spf-interval** • **timers throttle spf**



CHAPTER 25

OSPF Support for Fast Hello Packets

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration results in faster convergence in an Open Shortest Path First (OSPF) network.

Note It is recommended to use Bidirectional Forwarding Detection (BFD) instead of Fast Hello Packets.

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.

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 Support for Fast Hello Packets

OSPF must be already configured in the network or must be configured at the same time as the OSPF Support for Fast Hello Packets feature.

Information About OSPF Support for Fast Hello Packets

OSPF Hello Interval and Dead Interval

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non broadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

OSPF Fast Hello Packets

OSPF fast hello packets refer to hello packets being sent at intervals of less than 1 second. To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See the section OSPF Hello Interval and Dead Interval, on page 252.

OSPF fast hello packets are achieved by using the **ip ospf dead-interval** command. The dead interval is set to 1 second, and the hello-multiplier value is set to the number of hello packets you want to send during that 1 second, thus providing subsecond or "fast" hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

Benefits of OSPF Fast Hello Packets

The benefit of the OSPF Support for Fast Hello Packets feature is that your OSPF network will experience faster convergence time than it would without fast hello packets. This feature allows you to detect lost neighbors within 1 second. It is especially useful in LAN segments, where neighbor loss might not be detected by the Open System Interconnection (OSI) physical layer and data-link layer.

How to Configure OSPF Fast Hello Packets

Configuring OSPF Fast Hello Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf dead-interval minimal hello-multiplier** *multiplier*
5. **end**
6. **show ip ospf interface** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as 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 gigabitethernet 0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf dead-interval minimal hello-multiplier** *multiplier* **Example:** `Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5`	Sets the interval during which at least one hello packet must be received, or else the neighbor is considered down. • In the example, OSPF Support for Fast Hello Packets is enabled by specifying the **minimal** keyword and the **hello-multiplier** keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode. • Use this command when you are ready to exit configuration mode and save the configuration to the running configuration file.
Step 6	**show ip ospf interface** [*interface-type interface-number*] **Example:** `Router# show ip ospf interface gigabitethernet 0/0/1`	(Optional) Displays OSPF-related interface information. • The relevant fields that verify OSPF fast hello packets are indicated in the sample output following this table.

Examples

The following sample output verifies that OSPF Support for Fast Hello Packets is configured. In the line that begins with "Timer intervals configured," the hello interval is 200 milliseconds, the dead interval is 1 second, and the next hello packet is due in 76 milliseconds.

```
Router# show ip ospf interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet Address 172.16.1.2/24, Area 0
  Process ID 1, Router ID 172.17.0.2, Network Type BROADCAST, Cost:1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.17.0.2, Interface address 172.16.1.2
  Backup Designated router (ID) 172.16.0.1, Interface address 172.16.1.1
  Timer intervals configured, Hello 200 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 76 msec
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Configuration Examples for OSPF Support for Fast Hello Packets

Example OSPF Fast Hello Packets

The following example configures OSPF fast hello packets; the dead interval is 1 second and 5 hello packets are sent every second:

```
interface gigabitethernet 0/0/1
 ip ospf dead-interval minimal hello-multiplier 5
```

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
OSPFv3 External Path Preference Option	"*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

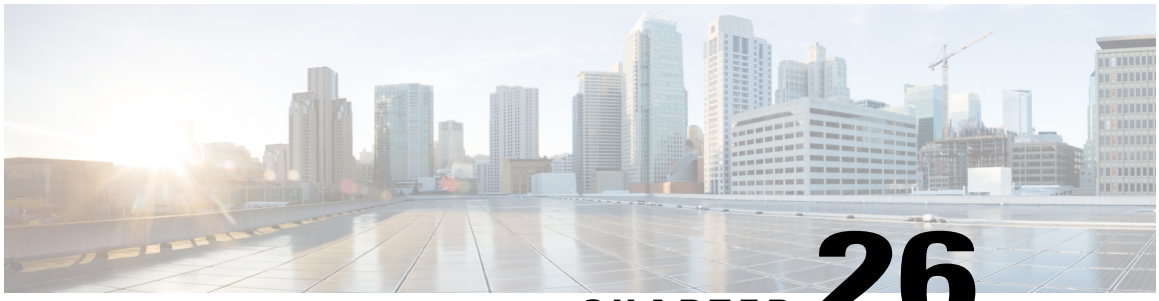
Feature Information for OSPF Support for Fast Hello Packets

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 28: Feature Information for OSPF Support for Fast Hello Packets

Feature Name	Releases	Feature Information
OSPF Support for Fast Hello Packets	Cisco IOS XE Release 2.1	The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration results in faster convergence in an Open Shortest Path First (OSPF) network.



CHAPTER 26

OSPF Incremental SPF

The Open Shortest Path First (OSPF) protocol can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event.

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.

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 Incremental SPF

It is presumed that you have OSPF configured in your network.

Information About OSPF Incremental SPF

OSPF uses Dijkstra's SPF algorithm to compute the shortest path tree (SPT). During the computation of the SPT, the shortest path to each node is discovered. The topology tree is used to populate the routing table with routes to IP networks. When changes to a Type-1 or Type-2 link-state advertisement (LSA) occur in an area, the entire SPT is recomputed. In many cases, the entire SPT need not be recomputed because most of the tree remains unchanged. Incremental SPF allows the system to recompute only the affected part of the tree. Recomputing only a portion of the tree rather than the entire tree results in faster OSPF convergence and saves CPU resources. Note that if the change to a Type-1 or Type-2 LSA occurs in the calculating router itself, then the full SPT is performed.

Incremental SPF is scheduled in the same way as the full SPF. Routers enabled with incremental SPF and routers not enabled with incremental SPF can function in the same internetwork.

How to Enable OSPF Incremental SPF

Enabling Incremental SPF

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **ispf**
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 1`	Configures an OSPF routing process.
Step 4	**ispf** **Example:** `Router(config-router)# ispf`	Enables incremental SPF.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Incremental SPF

Example Incremental SPF

This example enables incremental SPF:

```
router ospf 1
 ispf
```

Additional References

The following sections provide references related to OSPF Incremental SPF.

Related Documents

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF"
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
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

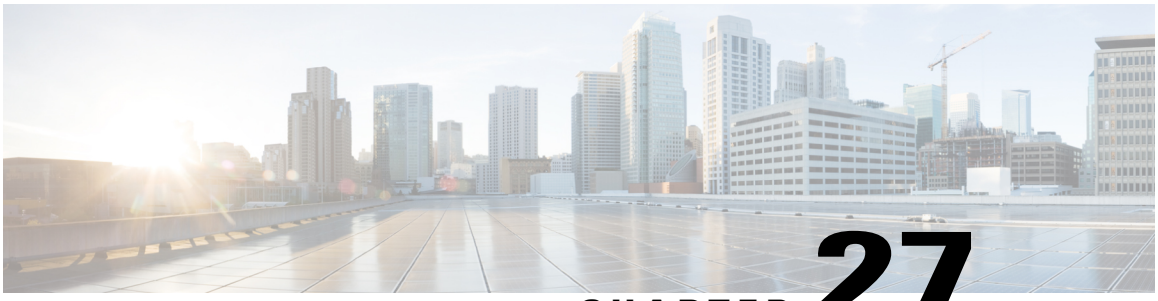
Feature Information for OSPF Incremental SPF

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 29: Feature Information for OSPF Incremental SPF

Feature Name	Releases	Feature Information
OSPF Incremental SPF	Cisco IOS XE Release 2.1	OSPF can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event The following commands are introduced or modified in the feature documented in this module: • **ispf**



CHAPTER 27

OSPF Limit on Number of Redistributed Routes

Open Shortest Path First (OSPF) supports a user-defined maximum number of prefixes (routes) that are allowed to be redistributed into OSPF from other protocols or other OSPF processes. Such a limit could help prevent the router from being flooded by too many redistributed routes.

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.

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 Limit on Number of Redistributed Routes

It is presumed that you have OSPF configured in your network, along with another protocol or another OSPF process you are redistributing.

Information About OSPF Limit on Number of Redistributed Routes

If large number of IP routes are sent into OSPF by redistributing Border Gateway Protocol (BGP) into OSPF, the network can be severely flooded. Limiting the number of redistributed routes prevents this potential problem.

OSPF can receive and accept packets from non-routable addresses (for example, 0.0.0.0/7) also.

How to Limit the Number of OSPF Redistributed Routes

This section contains the following procedures, which are mutually exclusive. That is, you cannot both limit redistributed prefixes and also choose to be warned.

Limiting the Number of Redistributed Routes

Note You cannot both limit redistributed prefixes and also choose to be warned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistribute maximum-prefix** *maximum* [*threshold*]
6. **end**
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	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router)# redistribute eigrp 10`	Redistributes routes from one routing domain into another routing domain.
Step 5	**redistribute maximum-prefix** *maximum* [*threshold*] **Example:** `Router(config-router)# redistribute maximum-prefix 100 80`	Sets a maximum number of IP prefixes that are allowed to be redistributed into OSPF. • There is no default value for the *maximum* argument. • The *threshold* value defaults to 75 percent. **Note** If the **warning-only** keyword had been configured in this command, no limit would be enforced; a warning message is simply logged.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.
Step 7	**show ip ospf** [*process-id*] **Example:** `Router# show ip ospf 1`	(Optional) Displays general information about OSPF routing processes. • If a redistribution limit was configured, the output will include the maximum limit of redistributed prefixes and the threshold for warning messages.

Requesting a Warning About the Number of Routes Redistributed into OSPF

Note You cannot both limit redistributed prefixes and also choose to be warned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistribute maximum-prefix** *maximum* [*threshold*] **warning-only**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**redistribute** *protocol* [*process-id*	*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router)# redistribute eigrp 10`	Redistributes routes from one routing domain into another routing domain.
Step 5	**redistribute maximum-prefix** *maximum* [*threshold*] **warning-only** **Example:** `Router(config-router)# redistribute maximum-prefix 1000 80 warning-only`	Causes a warning message to be logged when the maximum number of IP prefixes has been redistributed into OSPF. • Because the **warning-only** keyword is included, no limit is imposed on the number of redistributed prefixes into OSPF. • There is no default value for the *maximum* argument. • The *threshold* value defaults to 75 percent.

	Command or Action	Purpose
		• This example causes two warnings: one at 80 percent of 1000 (800 routes redistributed) and another at 1000 routes redistributed.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Limit on Number of Redistributed Routes

Example OSPF Limit the Number of Redistributed Routes

This example sets a maximum of 1200 prefixes that can be redistributed into OSPF process 1. Prior to reaching the limit, when the number of prefixes redistributed reaches 80 percent of 1200 (960 prefixes), a warning message is logged. Another warning is logged when the limit is reached and no more routes are redistributed.

```
router ospf 1
 router-id 10.0.0.1
 domain-id 5.6.7.8
 log-adjacency-changes
 timers lsa-interval 2
 network 10.0.0.1 0.0.0.0 area 0
 network 10.1.5.1 0.0.0.0 area 0
 network 10.2.2.1 0.0.0.0 area 0
 redistribute static subnets
 redistribute maximum-prefix 1200 80
```

Example Requesting a Warning About the Number of Redistributed Routes

This example allows two warning messages to be logged, the first if the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second if the number of redistributed routes reaches 600. However, the number of redistributed routes is not limited.

```
router ospf 1
 network 10.0.0.0 0.0.0.255 area 0
 redistribute eigrp 10 subnets
 redistribute maximum-prefix 600 85 warning-only
```

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*
OSPFv3 Address Families	*OSPFv3 Address Families* module

Standards

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

MIBs

MIBs	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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 5187.	*OSPFv3 Graceful Restart*

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

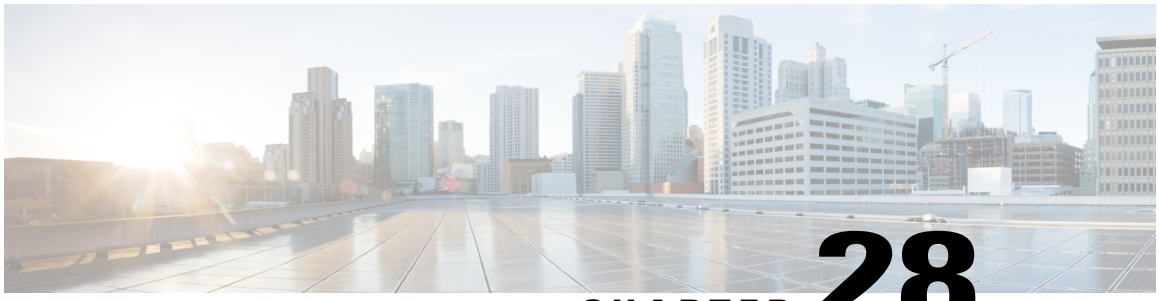
Feature Information for OSPF Limit on Number of Redistributed Routes

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 30: Feature Information for OSPF Limit on Number of Redistributed Routes

Feature Name	Releases	Feature Information
OSPF Limit on Number of Redistributed Routes	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	OSPF supports a user-defined maximum number of prefixes (routes) that are allowed to be redistributed into OSPF from other protocols or other OSPF processes. Such a limit could help prevent the router from being flooded by too many redistributed routes. The following commands are introduced or modified in the feature documented in this module: • **redistribute maximum-prefix** • **show ip ospf** • **show ip ospf database**



CHAPTER 28

OSPFv3 Fast Convergence: LSA and SPF Throttling

The Open Shortest Path First version 3 (OSPFv3) link-state advertisement (LSAs) and shortest-path first (SPF) throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability. It also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds.

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.

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 OSPFv3 Fast Convergence: LSA and SPF Throttling

Fast Convergence: LSA and SPF Throttling

The OSPFv3 LSA and SPF throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability. It also allows faster OSPFv3 convergence by providing LSA rate limiting in milliseconds.

OSPFv3 can use static timers for rate-limiting SPF calculation and LSA generation. Although these timers are configurable, the values used are specified in seconds, which poses a limitation on OSPFv3 convergence. LSA and SPF throttling achieves subsecond convergence by providing a more sophisticated SPF and LSA rate-limiting mechanism that is able to react quickly to changes and also provide stability and protection during prolonged periods of instability.

How to Configure OSPFv3 Fast Convergence: LSA and SPF Throttling

Tuning LSA and SPF Timers for OSPFv3 Fast Convergence

This task can be performed in Cisco IOS Release 15.1(3)S and 15.2(1)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. **timers lsa arrival** *milliseconds*
5. **timers pacing flood** *milliseconds*
6. **timers pacing lsa-group** *seconds*
7. **timers pacing retransmission** *milliseconds*

DETAILED STEPS

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

	Command or Action	Purpose
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 OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	**timers lsa arrival** *milliseconds* **Example:** `Device(config-rtr)# timers lsa arrival 300`	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.
Step 5	**timers pacing flood** *milliseconds* **Example:** `Device(config-rtr)# timers pacing flood 30`	Configures LSA flood packet pacing.
Step 6	**timers pacing lsa-group** *seconds* **Example:** `Device(config-router)# timers pacing lsa-group 300`	Changes the interval at which OSPFv3 LSAs are collected into a group and refreshed, checksummed, or aged.
Step 7	**timers pacing retransmission** *milliseconds* **Example:** `Device(config-router)# timers pacing retransmission 100`	Configures LSA retransmission packet pacing in IPv4 OSPFv3.

Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence

This task can be performed in releases prior to Cisco IOS Release 15.1(3)S and 15.2(1)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 router ospf** *process-id*
4. **timers throttle spf** *spf-start spf-hold spf-max-wait*
5. **timers throttle lsa** *start-interval hold-interval max-interval*
6. **timers lsa arrival** *milliseconds*
7. **timers pacing flood** *milliseconds*

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	**ipv6 router ospf** *process-id* **Example:** `Device(config)# ipv6 router ospf 1`	Enables OSPFv3 router configuration mode.
Step 4	**timers throttle spf** *spf-start spf-hold spf-max-wait* **Example:** `Device(config-rtr)# timers throttle spf 200 200 200`	Turns on SPF throttling.
Step 5	**timers throttle lsa** *start-interval hold-interval max-interval* **Example:** `Device(config-rtr)# timers throttle lsa 300 300 300`	Sets rate-limiting values for OSPFv3 LSA generation.
Step 6	**timers lsa arrival** *milliseconds* **Example:** `Device(config-rtr)# timers lsa arrival 300`	Sets the minimum interval at which the software accepts the same LSA from OSPFv3 neighbors.

	Command or Action	Purpose
Step 7	**timers pacing flood** *milliseconds* **Example:** `Device(config-rtr)# timers pacing flood 30`	Configures LSA flood packet pacing.

Configuration Examples for OSPFv3 Fast Convergence: LSA and SPF Throttling

Example: Configuring LSA and SPF Throttling for OSPFv3 Fast Convergence

The following example show how to display the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf

Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    ospf 2
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
```

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

Related Topic	Document Title
OSPFv3 Fast Convergence: LSA and SPF Throttling	"*OSPF Link-State Advertisement Throttling* " 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

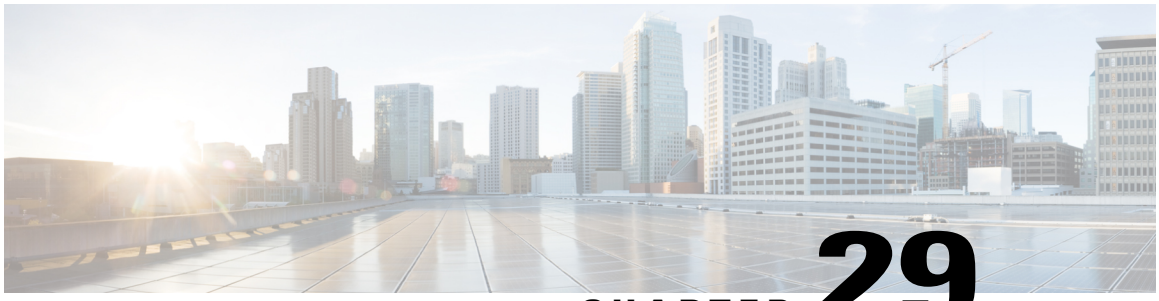
Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

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 31: Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

Feature Name	Releases	Feature Information
OSPFv3 Fast Convergence: LSA and SPF Throttling	Cisco IOS XE Release 2.1	The OSPFv3 LSA and SPF throttling feature provides a dynamic mechanism to slow down link-state advertisement updates in OSPFv3 during times of network instability.



CHAPTER 29

OSPFv3 Max-Metric Router LSA

The Open Shortest Path First version 3 (OSPFv3) max-metric router link-state advertisement (LSA) feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through the device if there are better alternate paths.

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.

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 OSPFv3 Max-Metric Router LSA

OSPFv3 Max-Metric Router LSA

The OSPFv3 max-metric router LSA feature enables OSPFv3 to advertise its locally generated router LSAs with a maximum metric. The feature allows OSPFv3 processes to converge but not attract transit traffic through

the device if there are better alternate paths. After a specified timeout or a notification from Border Gateway Protocol (BGP), OSPFv3 advertises the LSAs with normal metrics.

The max-metric LSA control places the OSPFv3 router into the stub router role using its LSA advertisement. A stub router only forwards packets destined to go to its directly connected links. In OSPFv3 networks, a device could become a stub router by advertising large metrics for its connected links, so that the cost of a path through this device becomes larger than that of an alternative path. OSPFv3 stub router advertisement allows a device to advertise the infinity metric (0xFFFF) for its connected links in router LSAs and advertise the normal interface cost if the link is a stub network.

How to Configure OSPFv3 Max-Metric Router LSA

Configuring the OSPFv3 Max-Metric Router LSA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **address-family ipv6 unicast**
5. **max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]]
6. **end**
7. **show ospfv3** [*process-id*] **max-metric**

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 OSPFv3 router configuration mode.

	Command or Action	Purpose
Step 4	**address-family ipv6 unicast** **Example:** `Device(config)# address-family ipv6 unicast`	Configures an instance of the OSPFv3 process in the IPv6 address family.
Step 5	**max-metric router-lsa** [**external-lsa** [*max-metric-value*]] [**include-stub**] [**inter-area-lsas** [*max-metric-value*]] [**on-startup** {*seconds* | **wait-for-bgp**}] [**prefix-lsa**] [**stub-prefix-lsa** [*max-metric-value*]] [**summary-lsa** [*max-metric-value*]] **Example:** `Device(config-router-af)# max-metric router-lsa on-startup wait-for-bgp`	Configures a device that is running the OSPFv3 protocol to advertise a maximum metric so that other devices do not prefer the device as an intermediate hop in their SPF calculations.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.
Step 7	**show ospfv3** [*process-id*] **max-metric** **Example:** `Device# show ospfv3 1 max-metric`	Displays OSPFv3 maximum metric origination information.

Configuration Examples for OSPFv3 Max-Metric Router LSA

Example: Verifying the OSPFv3 Max-Metric Router LSA

```
Router# show ipv6 ospf max-metric

           OSPFv3 Router with ID (192.1.1.1) (Process ID 1)

 Start time: 00:00:05.886, Time elapsed: 3d02h
 Originating router-LSAs with maximum metric
    Condition: always, State: active
```

Additional References for OSPF Nonstop Routing

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Configuring IETF NSF or Cisco NSF	"Configuring NSF-OSPF" module in the *Cisco IOS High Availability Configuration Guide*

Standard and RFCs

Standard/RFC	Title
RFC 2328	*OSPF Version 2*
RFC 3623	*Graceful OSPF Restart*

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

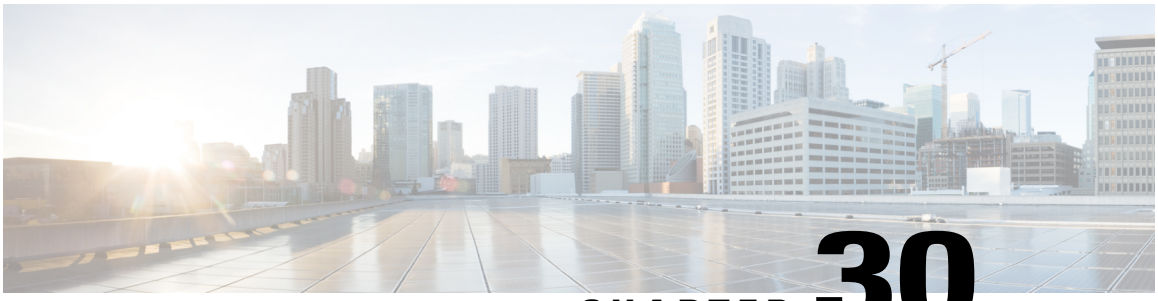
Feature Information for OSPFv3 Max-Metric Router LSA

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 32: Feature Information for OSPFv3 Max-Metric Router LSA

Feature Name	Releases	Feature Information
OSPFv3 Max-Metric Router LSA	Cisco IOS XE Release 3.4S	The OSPFv3 max-metric router LSA feature enables OSPF to advertise its locally generated router LSAs with a maximum metric. The following commands were introduced or modified: **max-metric router-lsa**, **show ipv6 ospf max-metric**, **show ospfv3 max-metric**.



CHAPTER 30

OSPF Link-State Advertisement Throttling

The OSPF Link-State Advertisement Throttling feature provides a dynamic mechanism to slow down link-state advertisement (LSA) updates in Open Shortest Path First (OSPF) during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds.

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.

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 LSA Throttling

It is presumed that you have OSPF configured in your network.

Information About OSPF LSA Throttling

Benefits of OSPF LSA Throttling

Prior to the OSPF LSA Throttling feature, LSA generation was rate-limited for 5 seconds. That meant that changes in an LSA could not be propagated in milliseconds, so the OSPF network could not achieve millisecond convergence.

The OSPF LSA Throttling feature is enabled by default and allows faster OSPF convergence (in milliseconds). This feature can be customized. One command controls the generation (sending) of LSAs, and another command controls the receiving interval. This feature also provides a dynamic mechanism to slow down the frequency of LSA updates in OSPF during times of network instability.

How OSPF LSA Throttling Works

The **timers throttle lsa all** command controls the generation (sending) of LSAs. The first LSA is always generated immediately upon an OSPF topology change, and the next LSA generated is controlled by the minimum start interval. The subsequent LSAs generated for the same LSA are rate-limited until the maximum interval is reached. The "same LSA" is defined as an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID.

The **timers lsa arrival** command controls the minimum interval for accepting the same LSA. If an instance of the same LSA arrives sooner than the interval that is set, the LSA is dropped. It is recommended that the arrival interval be less than or equal to the hold-time interval of the **timers throttle lsa all** command.

How to Customize OSPF LSA Throttling

Customizing OSPF LSA Throttling

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers throttle lsa all** *start-interval hold-interval max-interval*
5. **timers lsa arrival** *milliseconds*
6. **end**
7. **show ip ospf timers rate-limit**
8. **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* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**timers throttle lsa all** *start-interval hold-interval max-interval* **Example:** `Router(config-router)# timers throttle lsa all 100 10000 45000`	(Optional) Sets the rate-limiting values (in milliseconds) for LSA generation. • The default values are as follows: • *start-interval*is 0 milliseconds. • *hold-interval*is 5000 milliseconds. • *max-interval*is 5000 milliseconds.
Step 5	**timers lsa arrival** *milliseconds* **Example:** `Router(config-router)# timers lsa arrival 2000`	(Optional) Sets the minimum interval (in milliseconds) between instances of receiving the same LSA. • The default value is 1000 milliseconds. • We suggest you keep the *milliseconds*value of the LSA arrival timer less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

	Command or Action	Purpose

Step 7	**show ip ospf timers rate-limit**
	
	Example:
	`Router# show ip ospf timers rate-limit`
	
	Example:
	
	Example:
	`LSAID: 10.1.1.1 Type: 1 Adv Rtr: 172.16.2.2 Due in: 00:00:00.028`
	
	Example:
	`LSAID: 192.168.4.1 Type: 3 Adv Rtr: 172.17.2.2 Due in: 00:00:00.028`
		(Optional) Displays a list of the LSAs in the rate limit queue (about to be generated).
		• The example shows two LSAs in the queue. Each LSA is identified by LSA ID number, Type (of LSA), Advertising router ID, and the time in hours:minutes:seconds (to the milliseconds) when the LSA is due to be generated.

Step 8	**show ip ospf**
	
	Example:
	`Router# show ip ospf`
	
	Example:
	
	Example:
	`Routing Process "ospf 4" with ID 10.10.24.4`
	
	Example:
	`Supports only single TOS(TOS0) routes`
	
	Example:
	`Supports opaque LSA`
	
	Example:
	`Supports Link-local Signaling (LLS)`
	
	Example:
	`Initial SPF schedule delay 5000 msecs`
		(Optional) Displays information about OSPF.
		• The output lines that specify initial throttle delay, minimum hold time for LSA throttle, and maximum wait time for LSA throttle indicate the LSA throttling values.

	Command or Action	Purpose

	Example:
	`Minimum hold time between two consecutive SPFs 10000 msecs`
	Example:
	`Maximum wait time between two consecutive SPFs 10000 msecs`
	Example:
	`Incremental-SPF disabled`
	Example:
	`Initial LSA throttle delay 100 msecs`
	Example:
	`Minimum hold time for LSA throttle 10000 msecs`
	Example:
	`Maximum wait time for LSA throttle 45000 msecs`
	Example:
	`Minimum LSA arrival 1000 msecs`
	Example:
	`LSA group pacing timer 240 secs`
	Example:
	`Interface flood pacing timer 33 msecs`
	Example:
	`Retransmission pacing timer 66 msecs`
	Example:
	`Number of external LSA 0. Checksum Sum 0x0`	

	Command or Action	Purpose

	Example:
	`Number of opaque AS LSA 0. Checksum Sum 0x0`
	Example:
	`Number of DCbitless external and opaque AS LSA 0`
	Example:
	`Number of DoNotAge external and opaque AS LSA 0`
	Example:
	`Number of areas in this router is 1. 1 normal 0 stub 0 nssa`
	Example:
	`External flood list length 0`
	Example:
	`Area 24`
	Example:
	`Number of interfaces in this area is 2`
	Example:
	`Area has no authentication`
	Example:
	`SPF algorithm last executed 04:28:18.396 ago`
	Example:
	`SPF algorithm executed 8 times`
	Example:
	`Area ranges are`	

	Command or Action	Purpose

	Example:
	`Number of LSA 4. Checksum Sum 0x23EB9`
	Example:
	`Number of opaque link LSA 0. Checksum Sum 0x0`
	Example:
	`Number of DCbitless LSA 0`
	Example:
	`Number of indication LSA 0`
	Example:
	`Number of DoNotAge LSA 0`
	Example:
	`Flood list length 0`	

Configuration Examples for OSPF LSA Throttling

Example OSPF LSA Throttling

This example customizes OSPF LSA throttling so that the start interval is 200 milliseconds, the hold interval is 10,000 milliseconds, and the maximum interval is 45,000 milliseconds. The minimum interval between instances of receiving the same LSA is 2000 milliseconds.

```
router ospf 1
 log-adjacency-changes
 timers throttle lsa all 200 10000 45000
 timers lsa arrival 2000
 network 10.10.4.0 0.0.0.255 area 24
 network 10.10.24.0 0.0.0.255 area 24
```

Additional References

The following sections provide references related to OSPF LSA throttling.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF"
OSPFv3 Fast Convergence: LSA and SPF Throttling	"*OSPFv3 Fast Convergence: LSA and SPF Throttling*" module
OSPFv3 Max-Metric Router LSA	"*OSPFv3 Max-Metric Router LSA*" module

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

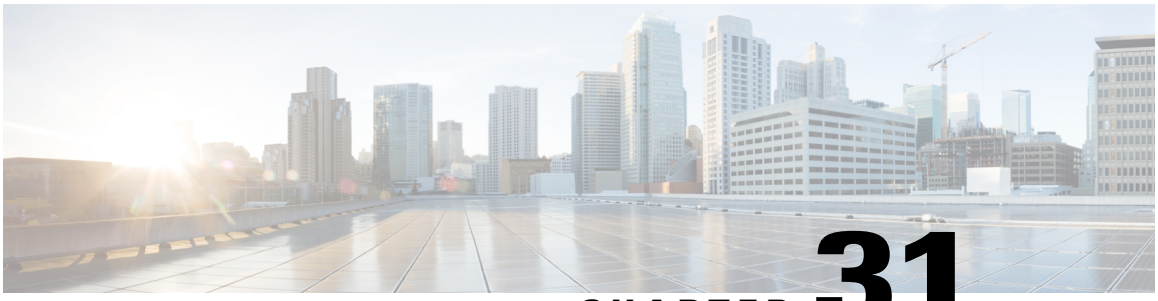
Feature Information for OSPF Link-State Advertisement Throttling

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 33: Feature Information for OSPF Link-State Advertisement Throttling

Feature Name	Releases	Feature Information
OSPF Link-State Advertisement Throttling	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	The OSPF Link-State Advertisement Throttling feature provides a dynamic mechanism to slow down link-state advertisement (LSA) updates in OSPF during times of network instability. It also allows faster OSPF convergence by providing LSA rate limiting in milliseconds. The following commands are introduced or modified in the feature documented in this module: • **debug ip ospf database-timer rate-limit** • **show ip ospf** • **show ip ospf timers rate-limit** • **timers lsa arrival** • **timers throttle lsa all**



CHAPTER 31

OSPF Support for Unlimited Software VRFs per PE Router

In a Multiprotocol Label Switching--Virtual Private Network (MPLS-VPN) deployment, each VPN routing and forwarding instance (VRF) needs a separate Open Shortest Path First (OSPF) process when configured to run OSPF. The OSPF Support for Unlimited Software VRFs per Provider Edge (PE) Router feature addresses the scalability issue for OSPF VPNs by eliminating the OSPF VPN limit of 32 processes.

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.

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 Support for Unlimited Software VRFs per PE Router

You must have OSPF configured in your network.

Restrictions for OSPF Support for Unlimited Software VRFs per PE Router

Only 32 processes per VRF can be supported. For different VRF processes, there is no limit.

Information About OSPF Support for Unlimited Software VRFs per PE Router

Before Cisco IOS Releases 12.3(4)T and 12.0(27)S, a separate OSPF process was necessary for each VRF that receives VPN routes via OSPF. When VPNs are deployed, an MPLS Provider Edge (PE) router will be running both multiprotocol Border Gateway Protocol (BGP) for VPN distribution, and Interior Gateway Protocol (IGP) for PE-P connectivity. OSPF is commonly used as the IGP between a customer edge (CE) router and a PE router. OSPF was not scalable in a VPN deployment because of the limit of 32 processes. By default, one process is used for connected routes and another process is used for static routes; therefore only 28 processes can be created for VRFs.

The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature allows for an approximate range of 300 to 10,000 VRFs, depending on the particular platform and on the applications, processes, and protocols that are currently running on the platform.

How to Configure OSPF Support for Unlimited Software VRFs per PE Router

Configuring Unlimited Software VRFs per PE Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vpn-name*
4. **exit**
5. **router ospf** *process-id* [**vrf** *vpn-name*]
6. **end**
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.
Step 3	**ip vrf** *vpn-name* **Example:** `Router(config)# ip vrf crf-1`	Defines a VPN routing and forwarding (VRF) instance and enters VRP configuration mode.
Step 4	**exit** **Example:** `Router(config-vrf)# exit`	Returns to global configuration mode.
Step 5	**router ospf** *process-id* [**vrf** *vpn-name*]	Enables OSPF routing.

	Command or Action	Purpose
	Example: `Router(config)# router ospf 1 vrf crf-1`	• The *process-id* argument identifies the OSPF process. • Use the **vrf** keyword and *vpn-name* argument to identify the VPN already defined in Step 3. **Note** You can now configure as many OSPF VRF processes as needed. Repeat Steps 3-5 as needed.
Step 6	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 7	**show ip ospf** [*process-id*] **Example:** `Router# show ip ospf 1`	Displays general information about OSPF routing processes.

Configuration Examples for OSPF Support for Unlimited Software VRFs per PE Router

Example Configuring OSPF Support for Unlimited Software VRFs per PE Router

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf first
Router(config-vrf)# exit
Router(config)# ip vrf second
Router(config-vrf)# exit
Router(config)# ip vrf third
Router(config-vrf)# exit
Router(config)# router ospf 12 vrf first
Router(config-router)# exit
Router(config)# router ospf 13 vrf second
Router(config-router)# exit
Router(config)# router ospf 14 vrf third
Router(config)# end
```

Example Verifying OSPF Support for Unlimited Software VRFs per PE Router

This example illustrates the output from the **show ip ospf** command to verify that OSPF VRF process 12 has been created for the VRF named first. The output that relates to the VRF first appears in bold.

```
Router# show ip ospf 12
main ID type 0x0005, value 0.0.0.100
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Connected to MPLS VPN Superbackbone, VRF first
 It is an area border router
 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 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 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 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:15.204 ago
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 1. Checksum Sum 0xD9F3
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Additional References

The following sections provide references related to the OSPF Support for Unlimited Software VRFs per Provider Edge Router feature.

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"

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

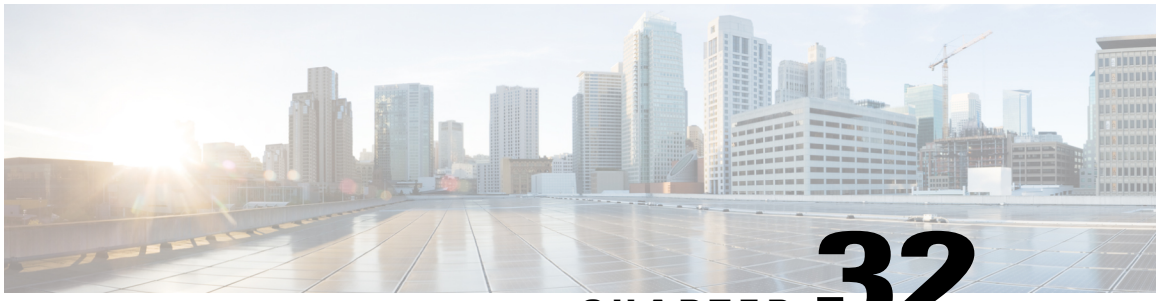
Feature Information for OSPF Support for Unlimited Software VRFs per PE Router

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 34: Feature Information for OSPF Support for Unlimited Software VRFs per Provider Edge Router

Feature Name	Releases	Feature Information
OSPF Support for Unlimited Software VRFs per Provider Edge Router	Cisco IOS XE Release 2.1	In a Multiprotocol Label Switching--Virtual Private Network (MPLS-VPN) deployment, each VPN routing and forwarding instance (VRF) needs a separate Open Shortest Path First (OSPF) process when configured to run OSPF. The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature addresses the scalability issue for OSPF VPNs by eliminating the OSPF VPN limit of 32 processes.



CHAPTER 32

OSPF Area Transit Capability

The OSPF Area Transit Capability feature provides an OSPF Area Border Router (ABR) with the ability to discover shorter paths through the transit area for forwarding traffic that would normally need to travel through the virtual-link path. This functionality allows Cisco IOS XE software to be compliant with RFC 2328, *OSPF Version 2*.

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.

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 Area Transit Capability

How the OSPF Area Transit Capability Feature Works

The OSPF Area Transit Capability feature is enabled by default. RFC 2328 defines OSPF area transit capability as the ability of the area to carry data traffic that neither originates nor terminates in the area itself. This capability enables the OSPF ABR to discover shorter paths through the transit area and to forward traffic along those paths rather than using the virtual link or path, which is not optimal.

For a detailed description of OSPF area transit capability, see RFC 2328, OSPF Version 2 .

How to Disable OSPF Area Transit Capability

Disabling OSPF Area Transit Capability on an Area Border Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **no capability transit**

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 100`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**no capability transit** **Example:** `Router(config-router)# no capability transit`	Disables OSPF area transit capability on all areas for a router process.

Additional References

The following sections provide references related to the OSPF Area Transit Capability feature.

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

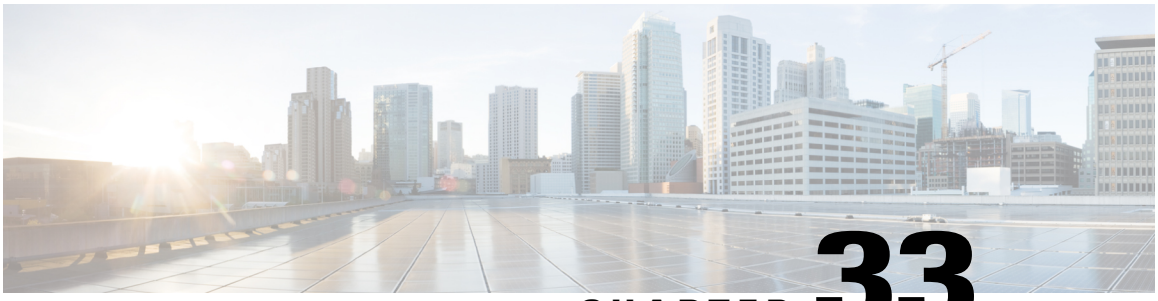
Feature Information for OSPF Area Transit Capability

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 35: Feature Information for OSPF Area Transit Capability

Feature Name	Releases	Feature Information
OSPF Area Transit Capability	Cisco IOS XE Release 2.1	The OSPF Area Transit Capability feature provides an OSPF Area Border Router (ABR) the ability to discover shorter paths through the transit area for forwarding traffic that would normally need to travel through the virtual-link path. This functionality allows Cisco IOS XE software to be compliant with RFC 2328. The command related to this feature is • **capability transit**



CHAPTER 33

OSPF Per-Interface Link-Local Signaling

The OSPF Per-Interface Link-Local Signaling feature allows you to selectively enable or disable Link-Local Signaling (LLS) for a specific interface regardless of the global (router level) setting that you have previously configured.

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.

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 Per-Interface Link-Local Signaling

LLS allows for the extension of existing OSPF packets in order to provide additional bit space. The additional bit space enables greater information per packet exchange between OSPF neighbors. This functionality is used, for example, by the OSPF Nonstop Forwarding (NSF) Awareness feature that allows customer premises equipment (CPE) routers that are NSF-aware to help NSF-capable routers perform nonstop forwarding of packets.

When LLS is enabled at the router level, it is automatically enabled for all interfaces. The OSPF Per-Interface Link-Local Signaling feature allows you to selectively enable or disable LLS for a specific interface. You may want to disable LLS on a per-interface basis depending on your network design. For example, disabling

LLS on an interface that is connected to a non-Cisco device that may be noncompliant with RFC 2328 can prevent problems with the forming of OSPF neighbors in the network.

How to Configure OSPF Per-Interface Link-Local Signaling

Turning Off LLS on a Per-Interface Basis

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot /port*
4. **ip address** *ip-address mask* [**secondary**]
5. **no ip directed-broadcast** [*access-list-number* | *extended access-list-number*]
6. **ip ospf message-digest-key** *key-id encryption-type* **md5** *key*
7. [**no** | **default**] **ip ospf lls** [**disable**]

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 slot /port* **Example:** `Router(config)# interface gigabitethernet 1/1/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* [**secondary**] **Example:** `Router(config-if)# ip address 10.2.145.20 255.255.255.0`	Sets a primary or secondary IP address for an interface.
Step 5	**no ip directed-broadcast** [*access-list-number* | *extended access-list-number*]	Drops directed broadcasts destined for the subnet to which that interface is attached, rather than broadcasting them.

	Command or Action	Purpose
	Example: `Router(config-if)# no ip directed-broadcast`	• The forwarding of IP directed broadcasts on Ethernet interface 1/0 is disabled.
Step 6	**ip ospf message-digest-key** *key-id encryption-type* **md5** *key* **Example:** `Router(config-if)# ip ospf message-digest-key 100 md5 testing`	Enables OSPF Message Digest 5 (MD5) algorithm authentication.
Step 7	[**no** | **default**] **ip ospf lls** [**disable**] **Example:** `Router(config-if)# ip ospf lls disable`	Disables LLS on an interface, regardless of the global (router level) setting.

What to Do Next

To verify that LLS has been enabled or disabled for a specific interface, use the **show ip ospf interface** command. See the "Example: Configuring and Verifying the OSPF Per-Interface Link-Local Signaling Feature" section for an example of the information displayed.

Configuration Examples for OSPF Per-Interface Link-Local Signaling

Example Configuring and Verifying OSPF Per-Interface Link-Local Signaling

In the following example, LLS has been enabled on GigabitEthernet interface 1/1/0 and disabled on GigabitEthernet interface 2/1/0:

```
interface gigabitethernet1/1/0
 ip address 10.2.145.2 255.255.255.0
 no ip directed-broadcast
 ip ospf message-digest-key 1 md5 testing
 ip ospf lls
!
interface gigabitethernet2/1/0
 ip address 10.1.145.2 255.255.0.0
 no ip directed-broadcast
 ip ospf message-digest-key 1 md5 testing
!
 ip ospf lls disable
interface Ethernet3/0
 ip address 10.3.145.2 255.255.255.0
```

```
 no ip directed-broadcast
!
router ospf 1
 log-adjacency-changes detail
 area 0 authentication message-digest
 redistribute connected subnets
 network 10.0.0.0 0.255.255.255 area 1
 network 10.2.3.0 0.0.0.255 area 1
```

In the following example, the **show ip ospf interface** command has been entered to verify that LLS has been enabled for GigabitEthernet interface 1/1/0 and disabled for GigabitEthernet interface 2/1/0:

```
Router# show ip ospf interface
GigabitEthernet1/1/0 is up, line protocol is up
  Internet Address 10.2.145.2/24, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.2.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.2.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
!   Supports Link-local Signaling (LLS)
Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 8
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
GigabitEthernet2/1/0 is up, line protocol is up
  Internet Address 10.1.145.2/16, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.1.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.1.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
!   Does not support Link-local Signaling (LLS)
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 45.2.2.3  (Designated Router)
    Suppress hello for 0 neighbor(s)
GigabitEthernet3/1/0 is up, line protocol is up
  Internet Address 10.3.145.2/24, Area 1
  Process ID 1, Router ID 10.22.222.2, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.2.2.3, Interface address 10.3.145.1
  Backup Designated router (ID) 10.22.222.2, Interface address 10.3.145.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
!   Supports Link-local Signaling (LLS)
Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Additional References

The following sections provide references related to the OSPF Per-Interface Link-Local Signaling feature.

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"
Configuring OSPF NSF Awareness	"Cisco Nonstop Forwarding"
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
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

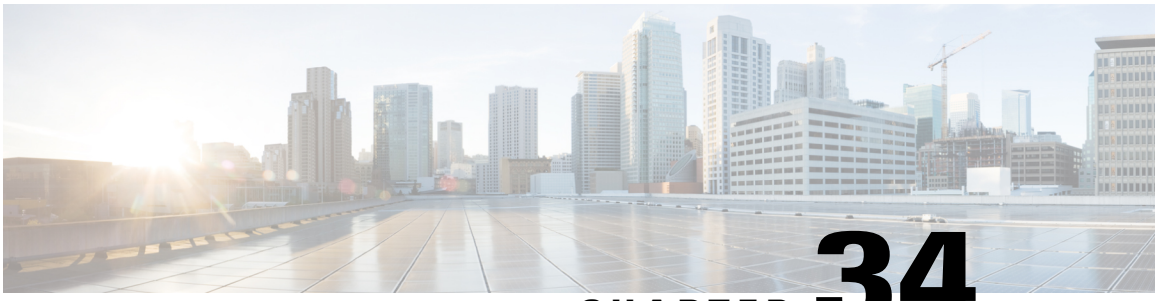
Feature Information for OSPF Per-Interface Link-Local Signaling

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 36: Feature Information for OSPF Per-Interface Link-Local Signaling

Feature Name	Releases	Feature Information
OSPF Per-Interface Link-Local Signaling	Cisco IOS XE Release 2.1	The OSPF Per-Interface Link-Local Signaling feature allows you to selectively enable or disable Link-Local Signaling (LLS) for a specific interface regardless of the global (router level) setting that you have previously configured. The following commands are introduced or modified in the feature documented in this module: • **ip ospf lls**



CHAPTER 34

OSPF Link-State Database Overload Protection

The OSPF Link-State Database Overload Protection feature allows you to limit the number of nonself-generated link-state advertisements (LSAs) for a given Open Shortest Path First (OSPF) process. Excessive LSAs generated by other routers in the OSPF domain can substantially drain the CPU and memory resources of the router.

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.

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 Link-State Database Overload Protection

It is presumed that you have OSPF running on your network.

Information About OSPF Link-State Database Overload Protection

Benefits of Using OSPF Link-State Database Overload Protection

The OSPF Link-State Database Overload Protection feature provides a mechanism at the OSPF level to limit the number of nonself-generated LSAs for a given OSPF process. When other routers in the network have been misconfigured, they may generate a high volume of LSAs, for instance, to redistribute large numbers of prefixes. This protection mechanism prevents routers from receiving a large number of LSAs and therefore experiencing CPU and memory shortages.

How OSPF Link-State Database Overload Protection Works

When the OSPF Link-State Database Overload Protection feature is enabled, the router keeps a count of the number of received (nonself-generated) LSAs that it has received. When the configured threshold number of LSAs is reached, an error message is logged. When the configured maximum number of LSAs is exceeded, the router will send a notification. If the count of received LSAs is still higher than the configured maximum after one minute, the OSPF process takes down all adjacencies and clears the OSPF database. In this ignore state, all OSPF packets received on any interface that belongs to this OSPF process are ignored and no OSPF packets are generated on any of these interfaces. The OSPF process remains in the ignore state for the time configured by the **ignore-time** keyword of the **max-lsa** command. Each time the OSPF process gets into an ignore state a counter is incremented. If this counter exceeds the number of minutes configured by the **ignore-count** keyword, the OSPF process stays permanently in the same ignore state and manual intervention is required to get the OSPF process out of the ignore state. The ignore state counter is reset to 0 when the OSPF process remains in the normal state of operation for the amount of time that was specified by the **reset-time** keyword.

If the **warning-only** keyword of the **max-lsa** command has been configured, the OSPF process will send only a warning that the LSA maximum has been exceeded.

How to Configure OSPF Link-State Database Overload Protection

Limiting the Number of Self-Generating LSAs for an OSPF Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **router-id** *ip-address*
5. **log -adjacency-changes** [**detail**]
6. **max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*]
7. **network** *ip-address wildcard-mask* **area** *area-id*
8. **end**
9. **show ip ospf** [*process-id area-id*] **database**[**database-summary**]

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* **Example:** `Router(config)# router ospf 1`	Enables OSPF routing. • The *process-id* argument identifies the OSPF process.
Step 4	**router-id** *ip-address* **Example:** `Router(config-router)# router-id 10.0.0.1`	Specifies a fixed router ID for an OSPF process.

	Command or Action	Purpose
Step 5	**log -adjacency-changes** [**detail**] **Example:** `Router(config-router)# log-adjacency-changes`	Configures the router to send a syslog message when an OSPF neighbor goes up or down.
Step 6	**max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*] **Example:** `Router(config-router)# max-lsa 12000`	Limits the number of nonself-generated LSAs that an OSPF routing process can keep in the OSPF link-state database (LSDB).
Step 7	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# network 209.165.201.1 255.255.255.255 area 0`	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.
Step 8	**end** **Example:** `Router(config-router)# end`	Ends the current configuration mode and returns to Privileged EXEC mode.
Step 9	**show ip ospf** [*process-id area-id*] **database**[**database-summary**] **Example:** `Router# show ip ospf 2000 database database-summary`	Displays lists of information related to the OSPF database for a specific router. • Use this command to verify the number of nonself-generated LSAs on a router.

Example

The **show ip ospf** command is entered with the **database-summary** keyword to verify the actual number of nonself-generated LSAs on a router. This command can be used at any time to display lists of information related to the OSPF database for a specific router.

```
Router# show ip ospf 2000 database database-summary

            OSPF Router with ID (192.168.1.3) (Process ID 2000)
Area 0 database summary
  LSA Type      Count    Delete   Maxage
  Router        5        0        0
  Network       2        0        0
  Summary Net   8        2        2
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
    Prefixes redistributed in Type-7  0
```

```
  Opaque Link    0         0         0
  Opaque Area    0         0         0
  Subtotal       15        2         2
Process 2000 database summary
  LSA Type       Count     Delete    Maxage
  Router         5         0         0
  Network        2         0         0
  Summary Net    8         2         2
  Summary ASBR   0         0         0
  Type-7 Ext     0         0         0
  Opaque Link    0         0         0
  Opaque Area    0         0         0
  Type-5 Ext     4         0         0
    Prefixes redistributed in Type-5  0
  Opaque AS      0         0         0
  Non-self       16
  Total          19        2         2
```

Configuration Examples for OSPF Link-State Database Overload Protection

Setting a Limit for LSA Generation Example

In the following example, the router is configured to not accept any more nonself-generated LSAs once a maximum of 14,000 has been exceeded:

```
Router(config)# router ospf 1
Router(config-router)# router-id 192.168.0.1
Router(config-router)# log-adjacency-changes
Router(config-router)# max-lsa 14000
Router(config-router)# area 33 nssa
Router(config-router)# network 192.168.0.1 0.0.0.0 area 1
Router(config-router)# network 192.168.5.1 0.0.0.0 area 1
Router(config-router)# network 192.168.2.1 0.0.0.0 area 0
```

In the following example, the **show ip ospf** command has been entered to confirm the configuration:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 0
It is an area border and autonomous system boundary router
```

In the following example, the following output appears when the **show ip ospf** command has been entered during the time when the router is in the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1
```

```
   Ignoring all neighbors due to max-lsa limit, time remaining: 00:04:52
It is an area border and autonomous system boundary router
```

The following output appears when the **show ip ospf** command has been entered after the router left the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1 - time remaining: 00:09:51
It is an area border and autonomous system boundary router
```

The following output appears when the **show ip ospf** command has been entered for a router that is permanently in the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 6
   Permanently ignoring all neighbors due to max-lsa limit
It is an area border and autonomous system boundary router
```

Additional References

The following sections provide references related to the OSPF Link-State Database Overload Protection feature.

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

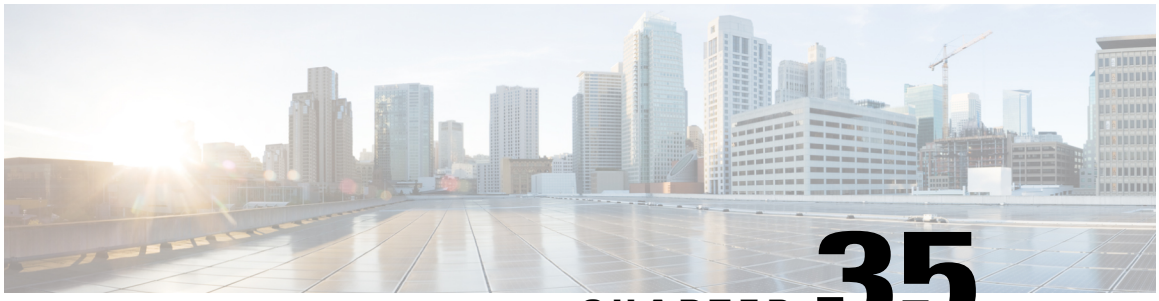
Feature Information for OSPF Link-State Database Overload Protection

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 37: Feature Information for OSPF Link-State Database Overload Protection

Feature Name	Releases	Feature Information
OSPF Link-State Database Overload Protection	Cisco IOS XE Release 2.1	The OSPF Link-State Database Overload Protection feature allows you to limit the number of nonself-generated link-state advertisements (LSAs) for a given OSPF process. Excessive LSAs generated by other routers in the OSPF domain can substantially drain the CPU and memory resources of the router. The following commands are introduced or modified in the feature documented in this module: • **max-lsa**



CHAPTER 35

OSPF MIB Support of RFC 1850 and Latest Extensions

The OSPF MIB Support of RFC 1850 and Latest Extensions feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring on the Open Shortest Path First (OSPF) routing protocol. Users have an improved ability to constantly monitor the changing state of an OSPF network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes. The protocol information collected by the OSPF MIB objects and trap objects can be used to derive statistics that will help monitor and improve overall network performance.

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.

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 MIB Support of RFC 1850 and Latest Extensions

- OSPF must be configured on the router.
- Simple Network Management Protocol (SNMP) must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.

Information About OSPF MIB Support of RFC 1850 and Latest Extensions

The following sections contain information about MIB objects standardized as part of RFC 1850 and defined in OSPF-MIB and OSPF-TRAP-MIB. In addition, extensions to RFC 1850 objects are described as defined in the two Cisco private MIBs, CISCO-OSPF-MIB and CISCO-OSPF-TRAP-MIB.

OSPF MIB Changes to Support RFC 1850

OSPF MIB

This section describes the new MIB objects that are provided by RFC 1850 definitions. These OSPF MIB definitions provide additional capacity that is not provided by the standard OSPF MIB that supported the previous RFC 1253. To see a complete set of OSPF MIB objects, see the OSPF-MIB file.

The table below shows the new OSPF-MIB objects that are provided by RFC 1850 definitions. The objects are listed in the order in which they appear within the OSPF-MIB file, per the tables that describe them.

Table 38: New OSPF-MIB Objects

OSPF-MIB Table	New MIB Objects
OspfAreaEntry table	• OspfAreaSummary • OspfAreaStatus
OspfStubAreaEntry	• OspfStubMetricType
OspfAreaRangeEntry	• OspfAreaRangeEffect
OspfHostEntry	• OspfHostAreaID

OSPF-MIB Table	New MIB Objects
OspfIfEntry	• OspfIfStatus • OspfIfMulticastForwarding • OspfIfDemand • OspfIfAuthType
OspfVirtIfEntry	• OspfVirtIfAuthType
OspfNbrEntry	• OspfNbmaNbrPermanence • OspfNbrHelloSuppressed
OspfVirtNbrEntry	• OspfVirtNbrHelloSuppressed
OspfExtLsdbEntry	• OspfExtLsdbType • OspfExtLsdbLsid • OspfExtLsdbRouterId • OspfExtLsdbSequence • OspfExtLsdbAge • OspfExtLsdbChecksum • OspfExtLsdbAdvertisement
OspfAreaAggregateEntry	• OspfAreaAggregateAreaID • OspfAreaAggregateLsdbType • OspfAreaAggregateNet • OspfAreaAggregateMask • OspfAreaAggregateStatusospfSetTrap • OspfAreaAggregateEffect

OSPF TRAP MIB

This section describes scalar objects and MIB objects that are provided to support RFC 1850.

The following scalar objects are added to OSPF-TRAP-MIB and are listed in the order in which they appear in the OSPF-TRAP-MIB file:

- OspfExtLsdbLimit
- OspfMulticastExtensions
- OspfExitOverflowInterval
- OspfDemandExtensions

The ospfSetTrap control MIB object contains the OSPF trap MIB objects that enable and disable OSPF traps in the IOS CLI. These OSPF trap MIB objects are provided by the RFC 1850 standard OSPF MIB. To learn how to enable and disable the OSPF traps, see the How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, on page 328.

The table below shows the OSPF trap MIB objects, listed in the order in which they appear within the OSPF-TRAP-MIB file.

Table 39: New OSPF-TRAP-MIB Objects

OSPF Control MIB Object	Trap MIB Objects
ospfSetTrap	• ospfIfStateChange • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrState • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure • ospfIfRxBadPacket • ospfVirtIfRxBadPacket • ospfTxRetransmit • ospfVirtIfTxRetransmit • ospfOriginateLsa • ospfMaxAgeLsa

CISCO OSPF MIB

This section describes scalar and Cisco-specific OSPF MIB objects that are provided as extensions to support the RFC 1850 OSPF MIB definitions, to provide capability that the standard MIB cannot provide.

The following scalar objects are added to OSPF-OSPF-MIB:

- cospfRFC1583Compatibility
- cospfOpaqueLsaSupport
- cospfOpaqueASLsaCount
- cospfOpaqueASLsaCksumSum

For each of the following table entries, the new Cisco-specific MIB objects that are provided as extensions to support the RFC 1850 OSPF MIB definitions are listed. To see the complete set of objects for the Cisco-specific OSPF MIB, refer to the CISCO-OSPF-MIB file.

The table below shows the new CISCO-OSPF-MIB objects that are provided by RFC 1850 definitions. The objects are listed in the order in which they appear within the CISCO-OSPF-MIB file, per the tables that describe them.

Table 40: New CISCO-OSPF-MIB Objects

CISCO-OSPF-MIB Table	New MIB Objects
cospfAreaEntry	• cospfOpaqueAreaLsaCount • cospfOpaqueAreaLsaCksumSum • cospfAreaNssaTranslatorRole • cospfAreaNssaTranslatorState • cospfAreaNssaTranslatorEvents
cospfLsdbEntry	• cospfLsdbType • cospfLsdbSequence • cospfLsdbAge • cospfLsdbChecksum • cospfLsdbAdvertisement
cospfIfEntry	• cospfIfLsaCount • cospfIfLsaCksumSum
cospfVirtIfEntry	• cospfVirtIfLsaCount • cospfVirtIfLsaCksumSum

CISCO-OSPF-MIB Table	New MIB Objects
cospfLocalLsdbEntry	• cospfLocalLsdbIpAddress • cospfLocalLsdbAddressLessIf • cospfLocalLsdbType • cospfLocalLsdbLsid • cospfLocalLsdbRouterId • cospfLocalLsdbSequence • cospfLocalLsdbAge • cospfLocalLsdbChecksum • cospfLocalLsdbAdvertisement
cospfVirtLocalLsdbEntry	• cospfVirtLocalLsdbTransitArea • cospfVirtLocalLsdbNeighbor • cospfVirtLocalLsdbType • cospfVirtLocalLsdbLsid • cospfVirtLocalLsdbRouterId • cospfVirtLocalLsdbSequence • cospfVirtLocalLsdbAge • cospfVirtLocalLsdbChecksum • cospfVirtLocalLsdbAdvertisement

CISCO OSPF TRAP MIB

The cospfSetTrap MIB object represents trap events in CISCO-OSPF-TRAP-MIB. This is a bit map, where the first bit represents the first trap. The following MIB objects are TRAP events that have been added to support RFC 1850. To see a complete set of Cisco OSPF Trap MIB objects, see the CISCO-OSPF-TRAP-MIB file.

The table below shows the trap events described within the cospfSetTrap MIB object in the CISCO-TRAP-MIB:

Table 41: CISCO-OSPF Trap Events

CISCO-OSPF-TRAP-MIB Trap Events	Trap Event Description
cospfIfConfigError	This trap is generated for mismatched MTU parameter errors that occur when nonvirtual OSPF neighbors are forming adjacencies.

CISCO-OSPF-TRAP-MIB Trap Events	Trap Event Description
cospfVirtIfConfigError	This trap is generated for mismatched MTU parameter errors when virtual OSPF neighbors are forming adjacencies.
cospfTxRetransmit	This trap is generated in the case of opaque LSAs when packets are sent by a nonvirtual interface. An opaque link-state advertisement (LSA) is used in MPLS traffic engineering to distribute attributes such as capacity and topology of links in a network. The scope of this LSA can be confined to the local network (Type 9, Link-Local), OSPF area (Type 20, Area-Local), or autonomous system (Type 11, AS scope). The information in an opaque LSA can be used by an external application across the OSPF network.
cospfVirtIfTxRetransmit	This trap is generated in the case of opaque LSAs when packets are sent by a virtual interface.
cospfOriginateLsa	This trap is generated when a new opaque LSA is originated by the router when a topology change has occurred.
cospfMaxAgeLsa	The trap is generated in the case of opaque LSAs.
cospfNssaTranslatorStatusChange	The trap is generated if there is a change in the ability of a router to translate OSPF type-7 LSAs into OSPF type-5 LSAs.

For information about how to enable OSPF MIB traps, see the How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, on page 328.

Benefits of the OSPF MIB

The OSPF MIBs (OSPF-MIB and OSPF-TRAP-MIB) and Cisco private OSPF MIBs (CISCO-OSPF-MIB and CISCO-OSPF-TRAP-MIB) allow network managers to more effectively monitor the OSPF routing protocol through the addition of new table objects and trap notification objects that previously were not supported by the RFC 1253 OSPF MIB.

New CLI commands have been added to enable SNMP notifications for OSPF MIB support objects, Cisco-specific errors, retransmission and state-change traps. The SNMP notifications are provided for errors and other significant event information for the OSPF network.

How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions

Enabling OSPF MIB Support

Before You Begin

Before the OSPF MIB Support of RFC 1850 and Latest Extensions feature can be used, the SNMP server for the router must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string1* **ro**
4. **snmp-server community** *string2* **rw**
5. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
6. **snmp-server enable traps ospf**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *string1* **ro** **Example:** `Router(config)# snmp-server community public ro`	Enables read access to all objects in the MIB, but does not allow access to the community strings.

	Command or Action	Purpose
Step 4	**snmp-server community** *string2* **rw** **Example:** `Router(config)# snmp-server community private rw`	Enables read and write access to all objects in the MIB, but does not allow access to the community strings.
Step 5	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 172.20.2.162 version 2c public ospf`	Specifies a recipient (target host) for SNMP notification operations. • If no *notification-type* is specified, all enabled notifications (traps or informs) will be sent to the specified host. • If you want to send only the OSPF notifications to the specified host, you can use the optional **ospf**keyword as one of the *notification-types*. (See the example.) Entering the **ospf** keyword enables the ospfSetTrap trap control MIB object.
Step 6	**snmp-server enable traps ospf** **Example:** `Router(config)# snmp-server enable traps ospf`	Enables all SNMP notifications defined in the OSPF MIBs. **Note** This step is required only if you wish to enable all OSPF traps. When you enter the **no snmp-server enable traps ospf** command, all OSPF traps will be disabled.
Step 7	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

What to Do Next

If you did not want to enable all OSPF traps, follow the steps in the following section to selectively enable one or more types of OSPF trap:

Enabling Specific OSPF Traps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ospf cisco-specific errors** [**config-error**] [**virt-config-error**]
4. **snmp-server enable traps ospf cisco-specific retransmit** [**packets**] [**virt-packets**]
5. **snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change**] [**shamlink-state-change**]
6. **snmp-server enable traps ospf cisco-specific lsa** [**lsa-maxage**] [**lsa-originate**]
7. **snmp-server enable traps ospf errors** [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**]
8. **snmp-server enable traps ospf lsa** [**lsa-maxage**] [**lsa-originate**]
9. **snmp-server enable traps ospf rate-limit** *seconds trap-number*
10. **snmp-server enable traps ospf retransmit** [**packets**] [**virt-packets**]
11. **snmp-server enable traps ospf state-change** [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps ospf cisco-specific errors** [**config-error**] [**virt-config-error**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific errors config-error`	Enables SNMP notifications for Cisco-specific OSPF configuration mismatch errors. • Entering the **snmp-server enable traps ospf cisco-specific errors** command with the optional **virt-config-error** keyword enables only the SNMP notifications for configuration mismatch errors on virtual interfaces.
Step 4	**snmp-server enable traps ospf cisco-specific retransmit** [**packets**] [**virt-packets**]	Enables error traps for Cisco-specific OSPF errors that involve re-sent packets.

	Command or Action	Purpose
	Example: `Router(config)# snmp-server enable traps ospf cisco-specific retransmit packets virt-packets`	• Entering the **snmp-server enable traps ospf cisco-specific retransmit** command with the optional **virt-packets**keyword enables only the SNMP notifications for packets that are re-sent on virtual interfaces.
Step 5	**snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change**] [**shamlink-state-change**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific state-change`	Enables all error traps for Cisco-specific OSPF transition state changes.
Step 6	**snmp-server enable traps ospf cisco-specific lsa** [**lsa-maxage**] [**lsa-originate**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific lsa`	Enables error traps for opaque LSAs.
Step 7	**snmp-server enable traps ospf errors** [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**] **Example:** `Router(config)# snmp-server enable traps ospf errors virt-config-error`	Enables error traps for OSPF configuration errors. • Entering the **snmp-server enable traps ospf errors** command with the optional **virt-config-error**keyword enables only the SNMP notifications for OSPF configuration errors on virtual interfaces.
Step 8	**snmp-server enable traps ospf lsa** [**lsa-maxage**] [**lsa-originate**] **Example:** `Router(config)# snmp-server enable traps ospf lsa`	Enables error traps for OSPF LSA errors.
Step 9	**snmp-server enable traps ospf rate-limit** *seconds trap-number* **Example:** `Router(config)# snmp-server enable traps ospf rate-limit 20 20`	Sets the rate limit for how many SNMP OSPF notifications are sent in each OSPF SNMP notification rate-limit window.
Step 10	**snmp-server enable traps ospf retransmit** [**packets**] [**virt-packets**]	Enables SNMP OSPF notifications for re-sent packets.

	Command or Action	Purpose
	Example: `Router(config)# snmp-server enable traps ospf retransmit`	
Step 11	**snmp-server enable traps ospf state-change** [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**] **Example:** `Router(config)# snmp-server enable traps ospf state-change`	Enables SNMP OSPF notifications for OSPF transition state changes.

Verifying OSPF MIB Traps on the Router

SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** [*options*] **Example:** `Router# show running-config | include traps`	Displays the contents of the currently running configuration file and includes information about enabled traps. • Verifies which traps are enabled.

Configuration Examples for OSPF MIB Support of RFC 1850 and Latest Extensions

Example Enabling and Verifying OSPF MIB Support Traps

The following example enables all OSPF traps.

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" chapter of the Cisco IOS XE Network Management Configuration Guide, *Release 2* .

Additional References

The following sections provide references related to the Area Command in Interface Mode for OSPFv2 feature.

Related Documents

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

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 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 OSPF MIB Support of RFC 1850 and Latest Extensions

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.

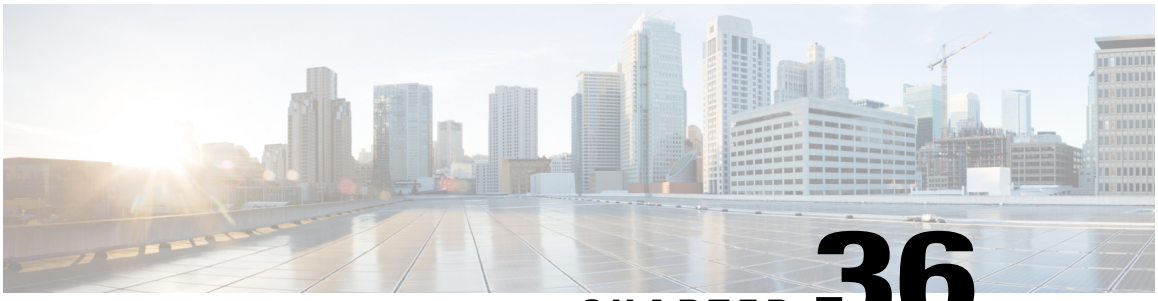
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 42: Feature Information for OSPF MIB Support of RFC 1850 and Latest Extensions

Feature Name	Releases	Feature Information
OSPF MIB Support of RFC 1850 and Latest Extensions	Cisco IOS XE Release 2.1	

Feature Name	Releases	Feature Information
		The OSPF MIB Support of RFC 1850 and Latest Extensions feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring on the Open Shortest Path First (OSPF) routing protocol. Users have an improved ability to constantly monitor the changing state of an OSPF network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes. The protocol information collected by the OSPF MIB objects and trap objects can be used to derive statistics that will help monitor and improve overall network performance. The following commands are introduced or modified in the feature documented in this module: • **snmp-server enable traps ospf** • **snmp-server enable traps ospf cisco-specific errors** • **snmp-server enable traps ospf cisco-specific lsa** • **snmp-server enable traps ospf cisco-specific retransmit** • **snmp-server enable traps ospf cisco-specific state-change** • **snmp-server enable traps ospf errors** • **snmp-server enable traps ospf lsa** • **snmp-server enable traps ospf rate-limit** • **snmp-server enable traps ospf retransmit**

Feature Name	Releases	Feature Information
		• snmp-server enable traps ospf state-change



CHAPTER 36

OSPF Enhanced Traffic Statistics

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.

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

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.
Step 2	**show ip ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ip ospf 10 traffic gigabitethernet 0/0/0`	Displays OSPFv2 traffic statistics.

	Command or Action	Purpose
Step 3	**clear ip ospf traffic** **Example:** `Router# clear ip ospf traffic`	Clears OSPFv2 traffic statistics.

Displaying and Clearing OSPF Traffic Statistics for OSPFv3

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`	Displays OSPFv3 traffic statistics.
Step 3	**clear ipv6 ospf traffic** **Example:** `Router# clear ipv6 ospf traffic`	Clears OSPFv3 traffic statistics.

Configuration Examples for OSPF Enhanced Traffic Statistics

Example Displaying and Clearing Enhanced Traffic Statistics for OSPFv2

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 GigabitEthernet0/0/1
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 Serial2/0/0
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 GigabitEthernet0/0/0
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
```

Example Displaying and Clearing Enhanced Traffic Statistics for OSPFv3

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 Serial2/0/0
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 GigabitEthernet0/0/0
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 Sham-Link MIB Support feature.

Related Documents

Related Topic	Document Title
Configuring OSPF sham-links	OSPF Sham-Link Support for MPLS VPN
SNMP configuration	*Cisco IOS Network Management Configuration Guide.*
SNMP commands	*Cisco IOS Network Management Command Reference.*

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

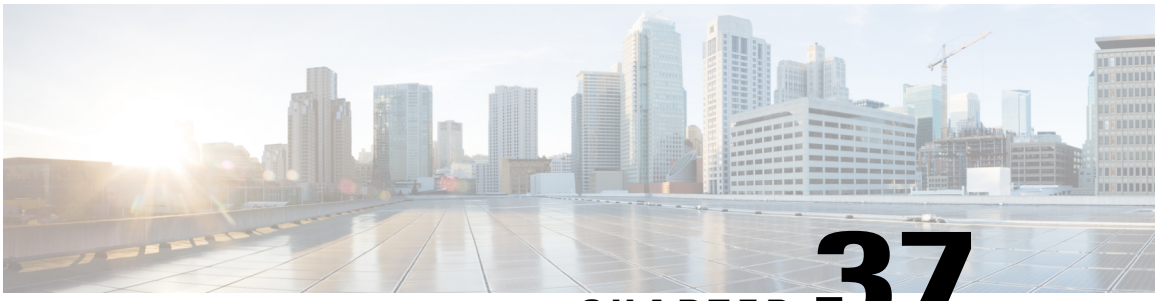
Feature Information for OSPF Enhanced Traffic Statistics

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 43: 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 XE Release 2.1	This document describes the detailed OSPF traffic statistics that are provided when the user enters the new and modified show commands for OSPFv2 and OSPFv3. The following commands are introduced or modified in the feature documented in this module: • **clear ipv6 ospf traffic** • **show ip ospf traffic** • **show ipv6 ospf traffic**



CHAPTER 37

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.

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

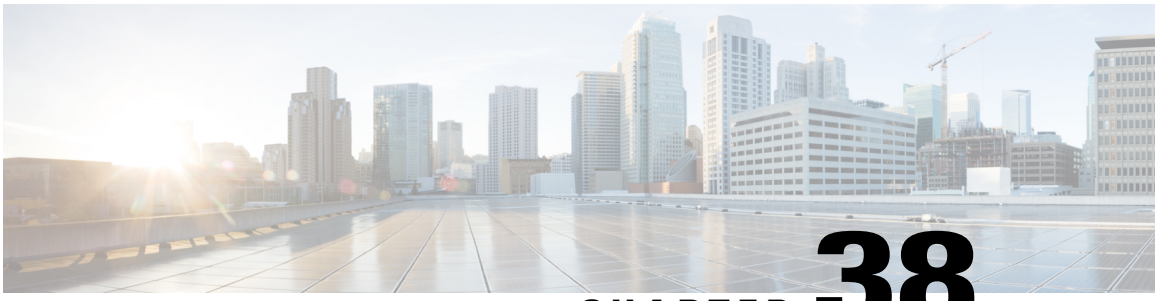
Feature Information for TTL Security Support for OSPFv3 on IPv6

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 44: TTL Security Support for OSPFv3 on IPv6

Feature Name	Software Releases	Feature Information
TTL Security Support for OSPFv3 on IPv6	Cisco IOS XE Release 3.7S	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**.



CHAPTER 38

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.

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:** `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 ospf** *process-id* **Example:** `Device(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:** `Device(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:** `Device(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: `Device> enable`	• 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 GigabitEthernet 0/0/0`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf ttl-security** [**hops** *hop-count* | **disable**] **Example:** `Device(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:** `Device(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:** `Device# 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:** `Device# 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:** `Device# 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:** `Device# 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:** `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	**interface** *type number* **Example:** `Device(config)#` **interface GigabitEthernet 0/1/0**	Configures an interface type and number and enters interface configuration mode.
Step 4	**ip ospf shutdown** **Example:** `Device(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:** `Device(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:** `Device#` **show ip ospf interface GigabitEthernet 0/1/0**	(Optional) Displays OSPF-related interface information.
Step 7	**show ip ospf [** *process-id* **]** **Example:** `Device#` **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

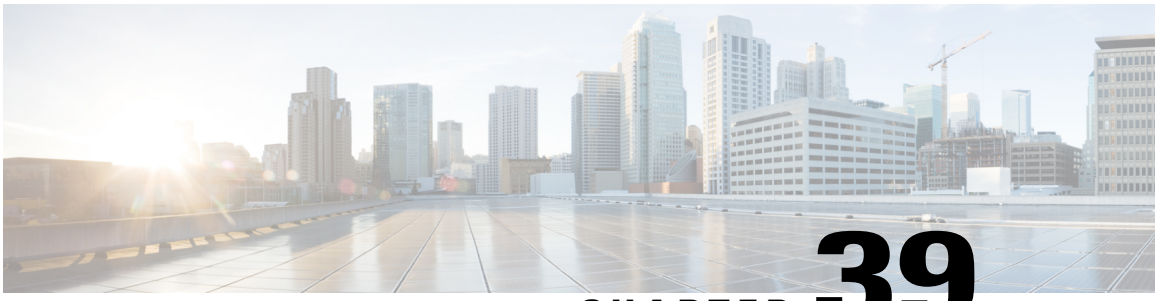
Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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 45: 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	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	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 39

OSPF Sham-Link MIB Support

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest 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.

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

Prerequisites for OSPF Sham-Link MIB Support

- It is presumed that you already have configured an OSPF sham-link.

- SNMP must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.

Restrictions for OSPF Sham-Link MIB Support

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

Information About OSPF Sham-Link MIB Support

OSPF Sham-Links in PE-PE Router Connections

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

Cisco OSPF MIB and Cisco OSPF Trap MIB Enhancements

The OSPF Sham-Link MIB Support feature introduces MIB support for OSPF sham-links through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New command-line interface (CLI) commands have been added to enable SNMP notifications for the OSPF sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface.

OSPF Sham-Link Configuration Support

The cospfShamLinksTable table object stores information about the sham-links that have been configured for the OSPF area. The cospfShamLinksTable allows access to the following MIB objects:

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

- cospfShamLinksEvents
- cospfShamLinksMetric

OSPF Sham-Link Neighbor Support

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

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

OSPF Sham-Link Interface Transition State Change Support

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

- ospfRouterId
- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksState

OSPF Sham-Link Neighbor Transition State Change Support

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

- ospfRouterId
- cospfShamLinkNbrArea

- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinkNbrIpAddrType
- cospfShamLinkNbrIpAddr
- cospfShamLinkNbrRtrId
- cospfShamLinkNbrState

Sham-Link Errors

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

- cospfShamLinkConfigError
- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

How to Configure OSPF Sham-Link MIB Support

Configuring the Router to Enable Sending of SNMP Notifications

SUMMARY STEPS

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

DETAILED STEPS

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

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

Enabling Sending of OSPF Sham-Link Error Traps

SUMMARY STEPS

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

DETAILED STEPS

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

Enabling OSPF Sham-Link Retransmissions Traps

SUMMARY STEPS

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

DETAILED STEPS

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

Enabling OSPF Sham-Link State Change Traps

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

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

Verifying OSPF Sham-Link MIB Traps on the Router

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config	include traps** **Example:** `Router# show running-config	include traps`	Displays the contents of the currently running configuration file and includes information about enabled traps. • Verifies if the trap is enabled.

Configuration Examples for OSPF Sham-Link MIB Support

Example Enabling and Verifying OSPF Sham-Link Error Traps

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

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

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

% Sham-link config error trap not enabled.
% Configure "cisco-specific errors config-error" first.
% This requirement allows both traps to be sent.
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# end
```

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific errors config-error
snmp-server enable traps ospf cisco-specific errors shamlink
```

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

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

Example Enabling and Verifying OSPF State Change Traps

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

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
```

Note that the **snmp-server enable traps ospf cisco-specific state-change shamlink** command enables the sham-link interface state change for the cospfShamLinksStateChange trap.

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

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

Example Enabling and Verifying OSPF Sham-Link Retransmissions Traps

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

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" part of the *Cisco IOS XE Network Management Configuration Guide, Release 2* .

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

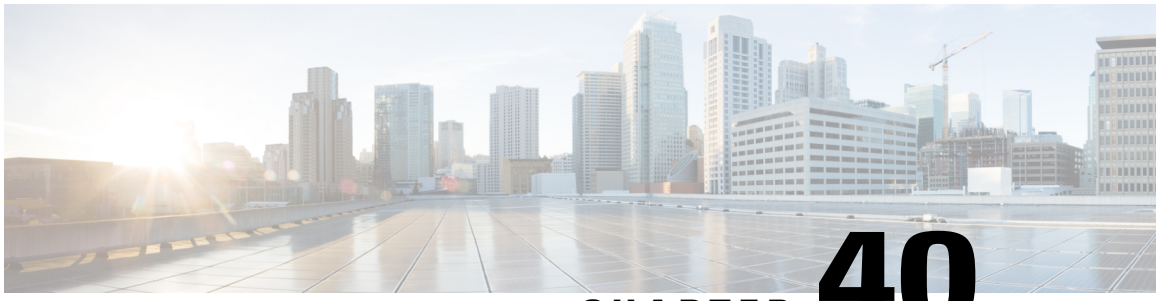
Feature Information for OSPF Sham-Link MIB Support

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

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

Table 46: Feature Information for OSPF Sham-Link MIB Support

Feature Name	Releases	Feature Information
OSPF Sham-Link MIB Support	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	This feature introduces MIB support for the OSPF Sham-Link feature through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and to the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New commands have been added to enable Simple Network Management Protocol (SNMP) notifications for the Open Shortest Path First (OSPF) sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface. The following commands are introduced or modified in the feature documented in this module: • **snmp-server enable traps ospf cisco-specific errors config-error** • **snmp-server enable traps ospf cisco-specific errors shamlink** • **snmp-server enable traps ospf cisco-specific retransmit** • **snmp-server enable traps ospf cisco-specific state-change.**



CHAPTER 40

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.

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:** `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	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:
	`Device(config)# router ospf 4`
	Example:
	Example:
	`Device(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:** `Device(config-router)# interface-id snmp-if-index`	Configures OSPF interfaces with the SNMP interface index identification numbers (ifIndex values).
Step 5	**end** **Example:** `Device(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:** `Device# show snmp mib ifmib ifindex GigabitEtherent 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.

```
Device# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# router ospf 1
Device(config-router)# interface-id snmp-if-index
Device(config-router)# ^Z
Device# 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
Device# 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:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ipv6 router ospf 1
Device(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:

```
Device# show snmp mib ifmib ifindex GigabitEthernet 0/0/0
0/0/0: Ifindex = 5
Device# 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)
Device# 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
Device# 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
Device# 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
Device# 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

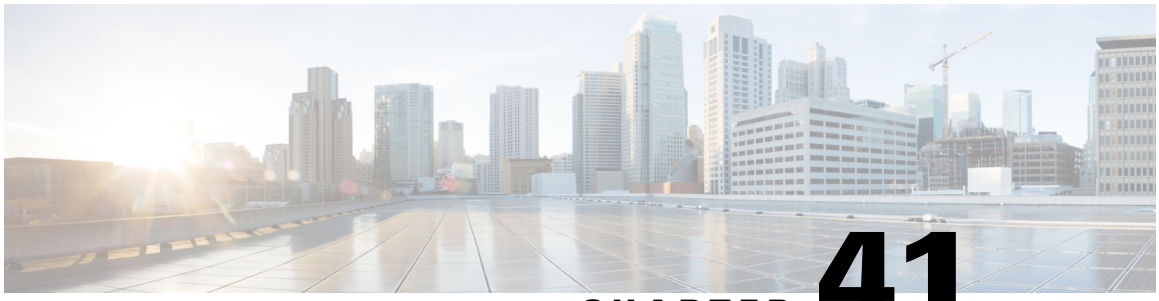
Feature Information for OSPF SNMP ifIndex Value for Interface ID

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 47: 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	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 41

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.

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:** `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 ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(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:** `Device(config-router)# local-rib-criteria forwarding-address`	Specifies that the OSPF local RIB will be used for route validation.
Step 5	**end** **Example:** `Device(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:** `Device# 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:** `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 ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**discard-route** [**external** [*distance*]] [**internal** [*distance*]] **Example:** `Device(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:** `Device(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:** `Device# 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.

```
Device# 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.

```
Device# 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.

```
Device# 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

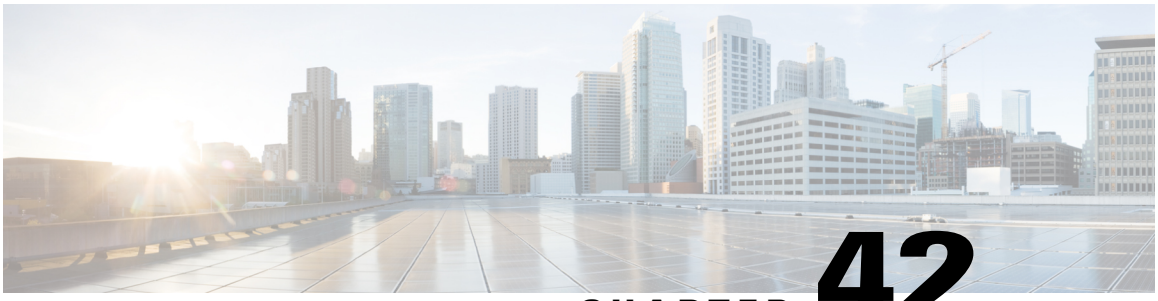
Feature Information for OSPFv2 Local RIB

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 48: Feature Information for the OSPFv2 Local RIB

Feature Name	Releases	Feature Information
OSPFv2 Local RIB	Cisco IOS XE Release 2.1	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 42

OSPF Support for Forwarding Adjacencies over MPLS TE Tunnels

The OSPF Support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels feature adds Open Shortest Path First (OSPF) support to the Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Forwarding Adjacency feature, which allows a network administrator to handle a traffic engineering, label-switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the shortest path first (SPF) algorithm. An OSPF forwarding adjacency can be created between routers in the same area.

History for the OSPF Support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels Feature

Release	Modification
12.0(24)S	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 series routers.

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.

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 Forwarding Adjacency

- OSPF must be configured in your network.
- Cisco Express Forwarding (CEF) must be enabled.
- You should understand MPLS TE tunnels for forwarding adjacency as described in the " MPLS Traffic Engineering Forwarding Adjacency" module.

Information About OSPF Forwarding Adjacency

OSPF includes MPLS TE tunnels in the OSPF link-state database in the same way that other links appear for purposes of routing and forwarding traffic. When an MPLS TE tunnel is configured between networking devices, that link is considered a forwarding adjacency. The user can assign a cost to the tunnel to indicate the link's preference. Other networking devices will see the tunnel as a link in addition to the physical link.

How to Configure OSPF Forwarding Adjacency

Configuring OSPF Forwarding Adjacency

Note Configure a forwarding adjacency on two LSP tunnels bidirectionally, from A to B and B to A. Otherwise, the forwarding adjacency is advertised, but not used in the IGP network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **mpls traffic-eng tunnels**
5. **interface loopback** *number*
6. **ip address** *ip-address mask*
7. **no shutdown**
8. **exit**
9. **interface tunnel** *number*
10. **tunnel mode mpls traffic-eng**
11. **tunnel mpls traffic-eng forwarding-adjacency** {**holdtime** *value*}
12. **ip ospf cost** *cost*
13. **exit**
14. **router ospf** *process-id*
15. **mpls traffic-eng router-id** *interface*
16. **mpls traffic-eng area** *number*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding (CEF).
Step 4	**mpls traffic-eng tunnels** **Example:** `Router(config)# mpls traffic-eng tunnels`	Enables MPLS traffic engineering tunnel signaling on a device.

	Command or Action	Purpose
Step 5	**interface loopback** *number* **Example:** `Router(config)# interface loopback0`	Configures a loopback interface and enters interface configuration mode. • Set up a loopback interface with a 32-bit mask, enable CEF, enable MPLS traffic engineering, and set up a routing protocol (OSPF) for the MPLS network.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.255`	Configures the IP address and subnet mask of the loopback interface.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 1`	Designates a tunnel interface for the forwarding adjacency and enters interface configuration mode.
Step 10	**tunnel mode mpls traffic-eng** **Example:** `Router(config-if)# tunnel mode mpls traffic-eng`	Sets the mode of a tunnel to MPLS for traffic engineering.
Step 11	**tunnel mpls traffic-eng forwarding-adjacency** {**holdtime** *value*} **Example:** `Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency holdtime 10000`	Advertises a TE tunnel as a link in an IGP network. • The **holdtime** *value* keyword argument combination is the time in milliseconds (ms) that a TE tunnel waits after going down before informing the network. The range is 0 to 4,294,967,295 ms. The default value is 0.
Step 12	**ip ospf cost** *cost* **Example:** `Router(config-if)# ip ospf cost 4`	(Optional) Configures the cost metric for a tunnel interface to be used as a forwarding adjacency.

	Command or Action	Purpose
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 14	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process and enters router configuration mode.
Step 15	**mpls traffic-eng router-id** *interface* **Example:** `Router(config-router)# mpls traffic-eng router-id ethernet 1/0`	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
Step 16	**mpls traffic-eng area** *number* **Example:** `Router(config-router)# mpls traffic-eng area 1`	Configures a router running OSPF MPLS so that it floods traffic engineering for the indicated OSPF area.
Step 17	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Forwarding Adjacency

Example OSPF Forwarding Adjacency

In the following example, the tunnel destination is the loopback interface on the other router. The router is configured with OSPF TE extensions and it floods traffic engineering link-state advertisements (LSAs) in OSPF area 0. The traffic engineering router identifier for the node is the IP address associated with Loopback 0. The last five lines of the example set up the routing protocol for the MPLS network, which is OSPF in this case.

Note Do not use the **mpls traffic-eng autoroute announce** command if you configure a forwarding adjacency in the tunnel.

```
ip routing
ip cef distributed
mpls traffic-eng tunnels
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
 no shutdown
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency holdtime 10000
 ip ospf cost 4
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth  10
 tunnel mpls traffic-eng path-option 2 dynamic
router ospf 5
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
 mpls traffic-eng router-id loopback0
 mpls traffic-eng area 0
```

When you look at the self-generated router LSA, you will see it as one of the links in router LSA (shown in bold in the following output).

```
Router# show ip ospf database route self-originate
OSPF Router with ID (10.5.5.5) (Process ID 5)
                Router Link States (Area 0)
  LS age:332
  Options:(No TOS-capability, DC)
  LS Type:Router Links
  Link State ID:10.5.5.5
  Advertising Router:10.5.5.5
  LS Seq Number:80000004
  Checksum:0x1D24
  Length:72
  Number of Links:4
    Link connected to another Router (point-to-point)
     (Link ID) Neighboring Router ID:10.3.3.3
     (Link Data) Router Interface address:0.0.0.23
      Number of TOS metrics:0
       TOS 0 Metrics:1562
    Link connected to:a Transit Network
     (Link ID) Designated Router address:172.16.0.1
     (Link Data) Router Interface address:172.16.0.2
      Number of TOS metrics:0
       TOS 0 Metrics:10
    Link connected to:a Transit Network
     (Link ID) Designated Router address:172.16.0.3
     (Link Data) Router Interface address:172.16.0.4
      Number of TOS metrics:0
       TOS 0 Metrics:10
    Link connected to:a Stub Network
     (Link ID) Network/subnet number:10.5.5.5
     (Link Data) Network Mask:255.255.255.255
      Number of TOS metrics:0
       TOS 0 Metrics:1
```

Additional References

The following sections provide references related to OSPF Forwarding Adjacency.

Related Documents

Related Topic	Document Title
MPLS traffic engineering forwarding adjacency	MPLS Traffic Engineering Forwarding Adjacency
Configuring OSPF for MPLS traffic engineering	MPLS Traffic Engineering and Enhancements
MPLS Traffic Engineering - LSP Attributes	MPLS Traffic Engineering - LSP Attributes

Standards

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

MIBs

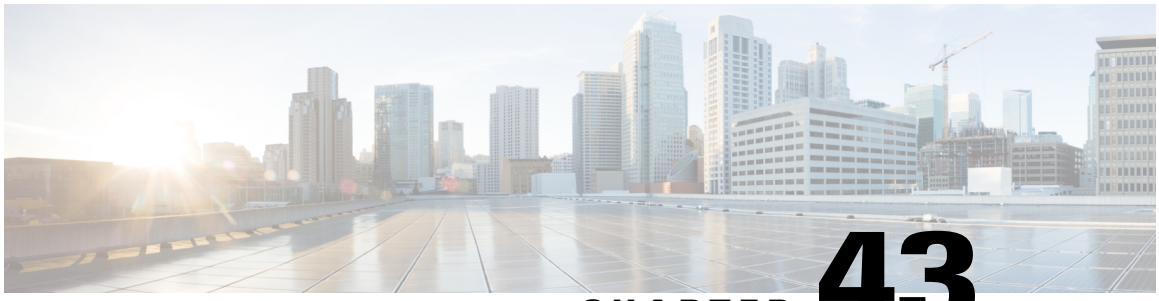
MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Technical Assistance

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



CHAPTER 43

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.

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: `Device> enable`	• 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 GigabitEthernet 0/2/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf** *process-id* **area** *area-id* [**secondaries none**] **Example:** `Device(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:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show ip ospf interface** [*type -number*] **Example:** `Device# show ip ospf interface GigabitEthernet 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:

```
Device(config)# interface GigabitEthernet 0/2/1
Device(config-if)# bandwidth 10000
```

```
Device(config-if)# ip address 172.16.1.1 255.255.255.0
Device(config-if)# ip ospf hello-interval 1
Device(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:

```
Device# show ip ospf interface GigabitEthernet 0/2/1
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

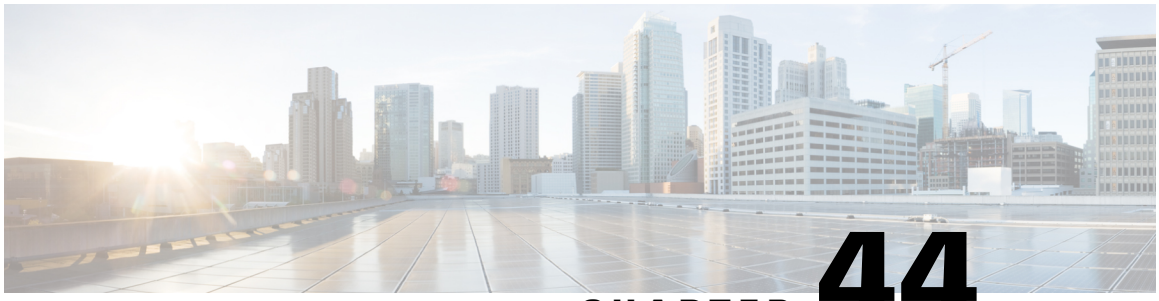
Feature Information for Enabling OSPFv2 on an Interface Basis

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 49: 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	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 44

OSPF Nonstop Routing

The OSPF Nonstop Routing feature allows a device with redundant Route Processors (RPs) to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned RP switchovers. The OSPF state is maintained by checkpointing the state information from OSPF on the active RP to the standby RP. After a switchover to the standby RP, OSPF uses the checkpointed information to continue operations without interruption.

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.

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 NSR

- OSPF NSR is available for platforms with redundant RPs or Cisco IOS software redundancy running Cisco IOS Release XE 3.3S or later releases.

Restrictions for OSPF NSR

- OSPF nonstop routing (NSR) can significantly increase the memory used by OSPF during certain phases of its operation. CPU usage also can be increased. You should be aware of router memory capacity and estimate the likely memory requirements of OSPF NSR. For more information see Configuring OSPF NSR. For routers where memory and CPU are constrained you might want to consider using OSPF NSF instead. For more information, see OSPF RFC 3623 Graceful Restart Helper Mode.
- A switchover from the active to the standby RP can take several seconds, depending on the hardware platform, and during this time OSPF is unable to send Hello packets. As a result, configurations that use small OSPF dead intervals might not be able to maintain adjacencies across a switchover.

Information About OSPFv3 Authentication Trailer

OSPF NSR Functionality

Although OSPF Nonstop Routing (NSR) serves a similar function to OSPF Nonstop Forwarding (NSF), it works differently. With NSF, OSPF on the newly active standby RP initially has no state information. OSPF uses extensions to the OSPF protocol to recover its state from neighboring OSPF devices. For the recovery to work, the neighbors must support the NSF protocol extensions and be willing to act as “helpers” to the device that is restarting. The neighbors must also continue forwarding data traffic to the device that is restarting while protocol state recovery takes place.

With NSR, by contrast, the device that performs the switchover preserves its state internally, and in most cases the neighbors are unaware of the switchover. Because assistance is not needed from neighboring devices, NSR can be used in situations where NSF cannot be used; for example, in networks where not all neighbors implement the NSF protocol extensions, or where network topology changes during the recovery making NSF unreliable, use NSR instead of NSF.

How to Configure OSPF Nonstop Routing

Configuring OSPF NSR

Perform this task to configure OSPF NSR.

NSR adds a single new line, "nsr," to the OSPF router mode configuration. Routers that do not support NSR, for whatever reason, will not accept this command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **nsr**
5. **end**
6. **show ip ospf [** *process-id* **] nsr [[objects]|[statistics]]**

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* **Example:** `Router(config)# router ospf 109`	Places the router in router configuration mode and configures an OSPF routing process.
Step 4	**nsr** **Example:** `Router(config-router)# nsr`	Configures NSR.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show ip ospf [** *process-id* **] nsr [[objects]|[statistics]]** **Example:** `Router# show ip ospf 109 nsr`	Displays OSPF NSR status information.

Troubleshooting Tips

OSPF NSR can increase the amount of memory used by the OSPF device process. To determine how much memory OSPF is currently using without NSR, you can use the **show processes** and **show processes memory** commands:

```
Device# show processes|include OSPF

 276 Mwe  133BE14         1900       1792    1060 8904/12000  0 OSPF-1 Router
 296 Mwe  133A824           10        971      10 8640/12000  0 OSPF-1 Hello
```

Process 276 is the OSPF device process that is to be checked. Use the **show processes memory** command to display its current memory use:

```
Device# show processes memory 276

Process ID: 276
Process Name: OSPF-1 Router
Total Memory Held: 4454800 bytes
```

In the above example, OSPF is using 4,454,800 bytes, or approximately 4.5 megabytes (MB). Because OSPF NSR can consume double this memory for brief periods, ensure that the device has at least 5 MB of free memory before enabling OSPF NSR.

Configuration Examples for OSPF Nonstop Routing

Example: Configuring OSPF NSR

The following example shows how to configure OSPF NSR:

```
Device> enable
Device# configure terminal
Device(config)# router ospf 1
Device(config-router)# nsr
Device(config-router)# end
Device# show ip ospf 1 nsr
Standby RP
 Operating in duplex mode
 Redundancy state: STANDBY HOT
 Peer redundancy state: ACTIVE
 ISSU negotation complete
 ISSU versions compatible
Routing Process "ospf 1" with ID 10.1.1.100
 NSR configured
 Checkpoint message sequence number: 3290
 Standby synchronization state: synchronized
 Bulk sync operations:  1
 Last sync start time:  15:22:48.971 UTC Fri Jan 14 2011
 Last sync finish time: 15:22:48.971 UTC Fri Jan 14 2011
 Last sync lost time:   -
 Last sync reset time:  -
 LSA Count: 2, Checksum Sum 0x00008AB4
```

The output shows that OSPF NSR is configured and that OSPF on the standby RP is fully synchronized and ready to continue operation should the active RP fail or if a manual switchover is performed.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF" in the *IP Routing: OSPF Configuration Guide*.
OSPFv2 loop-free alternate fast reroute	"OSPFv2 Loop-Free Alternate Fast Reroute" in the *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard/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

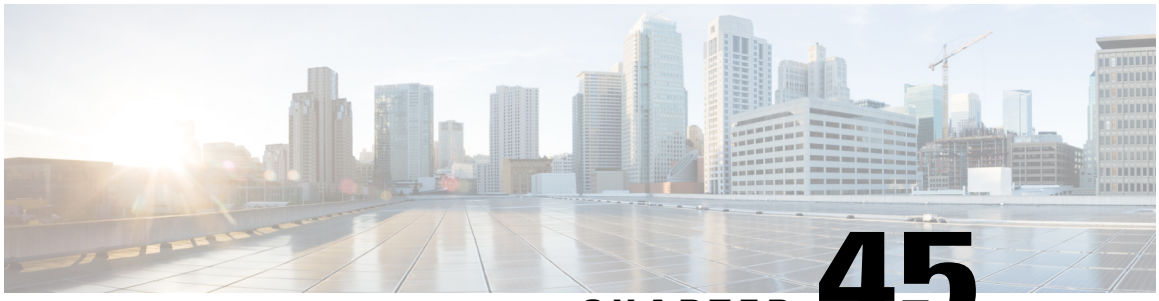
Feature Information for OSPF NSR

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 50: Feature Information for OSPF NSR

Feature Name	Releases	Feature Information
OSPF NSR	XE 3.3S Cisco IOS Release 15.1(1)SY	The OSPF NSR feature allows a router with redundant route processors to maintain its OSPF state and adjacencies across planned and unplanned RP switchovers. In Cisco IOS Release XE 3.3S, this feature was introduced. The following commands were introduced or modified: **nsr, show ip ospf nsr**.



CHAPTER 45

OSPFv3 NSR

The OSPFv3 NSR feature allows a router with redundant Route Processors (RPs) to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned RP switchovers. It does this by checkpointing state information from OSPFv3 on the active RP to the standby RP. Later, following a switchover to the standby RP, OSPFv3 can use this checkpointed information to continue operation without interruption.

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.

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 OSPFv3 NSR

OSPFv3 NSR Functionality

Although OSPFv3 NSR serves a similar function to the OSPFv3 graceful restart feature, it works differently. With graceful restart, OSPFv3 on the newly active standby RP initially has no state information, so it uses

extensions to the OSPFv3 protocol to recover its state from neighboring OSPFv3 devices. For this to work, the neighbors must support the graceful restart protocol extensions and be able to act as helpers to the restarting device. They must also continue forwarding data traffic to the restarting device while this recovery is taking place.

With NSR, by contrast, the device performing the switchover preserves its state internally, and in most cases the neighbors are unaware that anything has happened. Because no assistance is needed from neighboring devices, NSR can be used in situations where graceful restart cannot; for example, graceful restart is unreliable in networks where not all the neighbors implement the graceful restart protocol extensions or where the network topology changes during the recovery.

Note When NSR is enabled, the responsiveness and scalability of OSPF is degraded. The performance degradation happens because OSPF uses cpu and memory to checkpoint data to the standby Route Processor (RP).

How to Configure OSPFv3 NSR

Configuring OSPFv3 NSR

Perform this task to configure OSPFv3 NSR.

Note Devices that do not support NSR will not accept the **nsr** (OSPFv3) command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **nsr**
5. **end**
6. **show ospfv3** [*process-id*] [*address-family*] **nsr**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 109`	Places the device in router configuration mode and configures an OSPFv3 routing process.
Step 4	**nsr** **Example:** `Device(config-router)# nsr`	Configures NSR.
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.
Step 6	**show ospfv3** [*process-id*] [*address-family*] **nsr** **Example:** `Device# show ospfv3 109 nsr`	Displays OSPFv3 NSR status information.

Configuring OSPFv3 NSR for an Address Family

In address family configuration mode you can configure NSR for a particular address family. Perform this task to enable OSPFv3 NSR for an address family.

Note Devices that do not support NSR will not accept the **nsr** (OSPFv3) command.

SUMMARY STEPS

1. **router ospfv3** *process-id*
2. **address-family** {**ipv4** | **ipv6**} **unicast** [**vrf** *vrf-name*]
3. **nsr** [**disable**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 109`	Places the device in router configuration mode and configures an OSPFv3 routing process.
Step 2	**address-family** {**ipv4** | **ipv6**} **unicast** [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv4 unicast`	Enters IPv4 or IPv6 address family configuration mode for OSPFv3 router configuration mode.
Step 3	**nsr** [**disable**] **Example:** `Device(config-router-af)# nsr`	Enables NSR for the address family that is configured.

Disabling OSPFv3 NSR for an Address Family

In address family configuration mode the optional **disable** keyword is available for the **nsr** command. Perform this task to disable OSPFv3 NSR for an address family.

SUMMARY STEPS

1. **router ospfv3** *process-id*
2. **address-family** {**ipv4** | **ipv6**} **unicast** [**vrf** *vrf-name*]
3. **nsr** [**disable**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 109`	Places the device in router configuration mode and configures an OSPFv3 routing process.

	Command or Action	Purpose
Step 2	**address-family** {**ipv4** | **ipv6**} **unicast** [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast`	Enters IPv4 or IPv6 address family configuration mode for OSPFv3 router configuration mode.
Step 3	**nsr** [**disable**] **Example:** `Device(config-router-af)# nsr disable`	Disables NSR for the address family that is configured.

Troubleshooting Tips

OSPFv3 NSR can increase the amount of memory used by the OSPFv3 device process. To determine how much memory OSPFv3 is currently using without NSR, you can use the **show processes** and **show processes memory** commands:

```
Device# show processes
 | include OSPFv3
 276 Mwe  133BE14         1900       1792    1060 8904/12000  0 OSPFv3-1 Router
 296 Mwe  133A824           10        971      10 8640/12000  0 OSPFv3-1 Hello
```

Process 276 is the OSPFv3 device process that is to be checked. The **show processes memory** command is used to display its current memory use:

```
Device# show processes memory 276
Process ID: 276
Process Name: OSPFv3-1 Router
Total Memory Held: 4454800 bytes
```

In this case OSPFv3 is using 4,454,800 bytes or approximately 4.5 megabytes (MB). OSPFv3 NSR could double this for brief periods, so you should make sure the device has at least 5 MB of free memory before enabling OSPFv3 NSR.

Configuration Examples for OSPFv3 NSR

Example Configuring OSPFv3 NSR

The following example shows how to configure OSPFv3 NSR and verify that it is enabled:

```
Device(config)# router ospfv3 1
Device(config-router)# nsr
Device(config-router)# end
Device# show ospfv3 1
  OSPFv3 1 address-family ipv4
  Router ID 10.0.0.1
  Supports NSSA (compatible with RFC 3101)
```

```
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border and autonomous system boundary router
Redistributing External Routes from,
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
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
Retransmission limit dc 24 non-dc 24
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 3. 2 normal 0 stub 1 nssa
Non-Stop Routing enabled
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
   Area BACKBONE(0) (Inactive)
       Number of interfaces in this area is 1
       SPF algorithm executed 3 times
       Number of LSA 6. Checksum Sum 0x03C938
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 1
       Number of interfaces in this area is 3
       SPF algorithm executed 3 times
       Number of LSA 6. Checksum Sum 0x024041
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
   Area 3
       Number of interfaces in this area is 1
       It is a NSSA area
       Perform type-7/type-5 LSA translation
       SPF algorithm executed 4 times
       Number of LSA 5. Checksum Sum 0x024910
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0

OSPFv3 1 address-family ipv6
Router ID 10.0.0.1
Supports NSSA (compatible with RFC 3101)
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an area border and autonomous system boundary router
Redistributing External Routes from,
   ospf 2
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
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
Retransmission limit dc 24 non-dc 24
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 3. 2 normal 0 stub 1 nssa
Non-Stop Routing enabled
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
   Area BACKBONE(0) (Inactive)
       Number of interfaces in this area is 2
       SPF algorithm executed 2 times
       Number of LSA 6. Checksum Sum 0x02BAB7
```

```
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 1
        Number of interfaces in this area is 4
        SPF algorithm executed 2 times
        Number of LSA 7. Checksum Sum 0x04FF3A
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 3
        Number of interfaces in this area is 1
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        SPF algorithm executed 3 times
        Number of LSA 5. Checksum Sum 0x011014
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

The output shows that OSPFv3 NSR is configured.

Example Verifying OSPFv3 NSR

The following example shows how to verify OSPFv3 NSR status:

```
Device# show ospfv3 1 nsr
  Active RP
  Operating in duplex mode
  Redundancy state: ACTIVE
  Peer redundancy state: STANDBY HOT
  Checkpoint peer ready
  Checkpoint messages enabled
  ISSU negotiation complete
  ISSU versions compatible


          OSPFv3 1 address-family ipv4 (router-id 10.0.0.1)
  NSR configured
  Checkpoint message sequence number: 29
  Standby synchronization state: synchronized
  Bulk sync operations:  1
  Next sync check time:  12:00:14.956 PDT Wed Jun 6 2012
  LSA Count: 17, Checksum Sum 0x00085289


          OSPFv3 1 address-family ipv6 (router-id 10.0.0.1)
  NSR configured
  Checkpoint message sequence number: 32
  Standby synchronization state: synchronized
  Bulk sync operations:  1
  Next sync check time:  12:00:48.537 PDT Wed Jun 6 2012
  LSA Count: 18, Checksum Sum 0x0008CA05
```

The output shows that OSPFv3 NSR is configured and that OSPFv3 on the standby RP is fully synchronized and ready to continue operation if the active RP fails or if a manual switchover is performed.

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*
OSPFv3 Address Families	*OSPFv3 Address Families* module

Standards

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

MIBs

MIBs	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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
RFC 5187.	*OSPFv3 Graceful Restart*

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

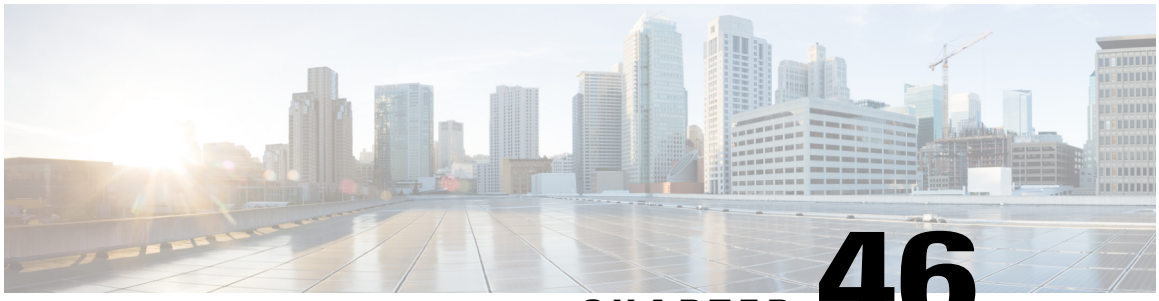
Feature Information for OSPFv3 NSR

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 51: Feature Information for OSPFv3 NSR

Feature Name	Releases	Feature Information
OSPFv3 NSR	15.1(2)SY 15.2(4)S	The OSPFv3 NSR feature allows a router with redundant RPs to maintain its OSPFv3 state and adjacencies across planned and unplanned RP switchovers. The following commands were introduced or modified: **clear ospfv3 nsr**, **nsr (OSPFv3)**, **show ospfv3 nsr**.



CHAPTER 46

OSPFv2 Loop-Free Alternate Fast Reroute

The OSPFv2 Loop-Free Alternate Fast Reroute feature uses a precomputed alternate next hop to reduce failure reaction time when the primary next hop fails. It lets you configure a per-prefix loop-free alternate (LFA) path that redirects traffic to a next hop other than the primary neighbor. The forwarding decision is made and service is restored without other routers' knowledge of the failure.

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.

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 Loop-Free Alternate Fast Reroute

Open Shortest Path First (OSPF) supports IP FRR only on platforms that support this feature in the forwarding plane. See the Cisco Feature Navigator, http://www.cisco.com/go/cfn , for information on platform support. An account on Cisco.com is not required.

Restrictions for OSPFv2 Loop-Free Alternate Fast Reroute

The OSPFv2 Loop-Free Alternate Fast Reroute feature is not supported on routers that are virtual links headends.

The OSPFv2 Loop-Free Alternate Fast Reroute feature is supported only in global VPN routing and forwarding (VRF) OSPF instances.

You cannot configure a traffic engineering (TE) tunnel interface as a protected interface. Use the MPLS Traffic Engineering--Fast Reroute Link and Node Protection feature to protect these tunnels. See the "MPLS Traffic Engineering--Fast Reroute Link and Node Protection" section in the *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* for more information.

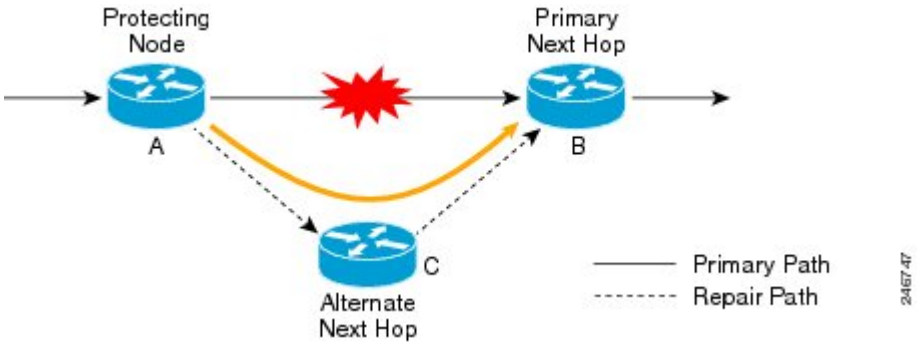
You can configure a TE tunnel interface in a repair path, but OSPF will not verify the tunnel's placement; you must ensure that it is not crossing the physical interface it is intended to protect.

Not all routes can have repair paths. Multipath primary routes might have repair paths for all, some, or no primary paths, depending on network topology, the connectivity of the computing router, and the attributes required of repair paths.

Information About OSPFv2 Loop-Free Alternate Fast Reroute

LFA Repair Paths

The figure below shows how the OSPFv2 Loop-Free Alternate Fast Reroute feature reroutes traffic if a link fails. A protecting router precomputes per-prefix repair paths and installs them in the global Routing Information Base (RIB). When the protected primary path fails, the protecting router diverts live traffic from the primary path to the stored repair path, without other routers' having to recompute network topology or even be aware that the network topology has changed.



LFA Repair Path Attributes

When a primary path fails, many paths are possible repair candidates. The OSPFv2 Loop-Free Alternate Fast Reroute feature default selection policy prioritizes attributes in the following order:

1 srlg

2 primary-path

3 interface-disjoint

4 lowest-metric

5 linecard-disjoint

6 node-protecting

7 broadcast-interface-disjoint

If the evaluation does not select any candidate, the repair path is selected by implicit load balancing. This means that repair path selection varies depending on prefix.

You can use the **show ip ospf fast-reroute** command to display the current configuration.

You can use the **fast-reroute tie-break** command to configure one or more of the repair-path attributes described in the following sections to select among the candidates:

Shared Risk Link Groups

A shared risk link group (SRLG) is a group of next-hop interfaces of repair and protected primary paths that have a high likelihood of failing simultaneously. The OSPFv2 Loop-Free Alternate Fast Reroute feature supports only SRLGs that are locally configured on the computing router. VLANs on a single physical interface are an example of an SRLG. If the physical interface fails, all the VLAN interfaces will fail at the same time. The default repair-path attributes might result in the primary path on one VLAN being protected by a repair path over another VLAN. You can configure the srlg attribute to specify that LFA repair paths do not share the same SRLG ID as the primary path. Use the **srlg** command to assign an interface to an SRLG.

Interface Protection

Point-to-point interfaces have no alternate next hop for rerouting if the primary gateway fails. You can set the interface-disjoint attribute to prevent selection of such repair paths, thus protecting the interface.

Broadcast Interface Protection

LFA repair paths protect links when a repair path and a protected primary path use different next-hop interfaces. However, on broadcast interfaces, if the LFA repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the node is protected but the link might not be. You can set the broadcast-interface-disjoint attribute to specify that the repair path never crosses the broadcast network the primary path points to; that is, it cannot use the interface and the broadcast network connected to it.

See " Broadcast and Non-Broadcast Multi-Access (NBMA) Links " in RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates* for information on network topologies that require this tiebreaker.

Node Protection

The default repair-path attributes might not protect the router that is the next hop in a primary path. You can configure the node-protecting attribute to specify that the repair path will bypass the primary-path gateway router.

Downstream Path

In the case of a high-level network failure or multiple simultaneous network failures, traffic sent over an alternate path might loop until OSPF recomputes the primary paths. You can configure the downstream attribute to specify that the metric of any repair path to the protected destination must be lower than that of the protecting node to the destination. This might result in lost traffic but it prevents looping.

Line-Card Disjoint Interfaces

Line-card interfaces are similar to SRLGs because all interfaces on the same line card will fail at the same time if there is a problem with the line card, for example, line card online insertion and removal (OIR). You can configure the linecard-disjoint attribute to specify that LFA repair paths use different interfaces than those on the primary-path line card.

Metric

An LFA repair path need not be the most efficient of the candidates. A high-cost repair path might be considered more attractive if it provides protection against higher-level network failures. You can configure the metric attribute to specify a repair-path policy that has the lowest metric.

Equal-Cost Multipath Primary Paths

Equal-cost multipath paths (ECMPs) found during the primary shortest path first (SPF) repair, might not be desirable in network designs where traffic is known to exceed the capacity of any single link. You can configure the primary-path attribute to specify an LFA repair path from the ECMP set, or the secondary-path attribute to specify an LFA repair path that is not from the ECMP set.

Candidate Repair-Path Lists

When OSPF computes a repair path, it keeps in the local RIB only the best from among all the candidate paths, in order to conserve memory. You can use the **fast-reroute keep-all-paths** command to create a list of all the candidate repair paths that were considered. This information can be useful for troubleshooting but it can greatly increase memory consumption so it should be reserved for testing and debugging.

How to Configure OSPFv2 Loop-Free Alternate Fast Reroute

Enabling Per-Prefix OSPFv2 Loop-Free Alternate Fast Reroute

Perform this task to enable per-prefix OSPFv2 Loop-Free Alternate Fast Reroute and select the prefix priority in an OSPF area.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix enable prefix-priority** *priority-level*
5. **exit**

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* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix enable prefix-priority** *priority-level* **Example:** `Router (config-router)# fast-reroute per-prefix enable prefix-priority low`	Enables repair-path computation and selects the priority level for repair paths. • Low priority specifies that all prefixes have the same eligibility for protection. High priority specifies that only high-priority prefixes are protected.
Step 5	**exit** **Example:** `Router (config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Specifying Prefixes to Be Protected by LFA FRR

Perform this task to specify which prefixes will be protected by LFA FRR. Only prefixes specified in the route map will be protected.

Note Only the following three match keywords are recognized in the route map: **match tag**, **match route-type**, and **match ip address prefix-list**.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [permit | deny] [*sequence-number*]
4. **match tag** *tag-name*
5. **exit**
6. **router ospf** *process-id*
7. **prefix-priority** *priority-level* **route-map** *map-tag*
8. **exit**

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	**route-map** *map-tag* [permit	deny] [*sequence-number*] **Example:** `Router(config)# route-map OSPF-PREFIX-PRIORITY`	Enters route-map configuration mode and specifies the map name.
Step 4	**match tag** *tag-name* **Example:** `Router(config-route-map)# match tag 886`	Specifies the prefixes to be matched. • Only prefixes that match the tag will be protected.
Step 5	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 7	**prefix-priority** *priority-level* **route-map** *map-tag* **Example:** `Router(config-router)# prefix-priority high route-map OSPF-PREFIX-PRIORITY`	Sets the priority level for repair paths and specifies the route map that defines the prefixes.
Step 8	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Configuring a Repair Path Selection Policy

Perform this task to configure a repair path selection policy, specifying a tiebreaking condition. See the LFA Repair Path Attributes, on page 434 for information on tiebreaking attributes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix tie-break** *attribute* **[required] index** *index-level*
5. **exit**

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	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix tie-break** *attribute* **[required] index** *index-level* **Example:** `Router(config-router)# fast-reroute per-prefix tie-break srlg required index 10`	Configures a repair path selection policy by specifying a tiebreaking condition and setting its priority level.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Creating a List of Repair Paths Considered

Perform this task to create a list of paths considered for LFA FRR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute keep-all-paths**
5. **exit**

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	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute keep-all-paths** **Example:** `Router(config-router)# fast-reroute keep-all-paths`	Specifies creating a list of repair paths considered for LFA FRR.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Prohibiting an Interface From Being Used as the Next Hop

Perform this task to prohibit an interface from being used as the next hop in a repair path.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf fast-reroute per-prefix candidate disable**
5. **exit**

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 GigabitEthernet 0/0/0`	Enters interface configuration mode for the interface specified.
Step 4	**ip ospf fast-reroute per-prefix candidate disable** **Example:** `Router(config-if)# ip ospf fast-reroute per-prefix candidate disable`	Prohibits the interface from being used as the next hop in a repair path.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuration Examples for OSPFv2 Loop-Free Alternate Fast Reroute

Example Enabling Per-Prefix LFA IP FRR

The following example shows how to enable per-prefix OSPFv2 Loop-Free Alternate Fast Reroute and select the prefix priority in an OSPF area:

```
Router(config)# router ospf 10
fast-reroute per-prefix enable prefix-priority low
```

Example Specifying Prefix-Protection Priority

The following example shows how to specify which prefixes will be protected by LFA FRR:

```
Router(config)# router ospf 10
prefix-priority high route-map OSPF-PREFIX-PRIORITY
fast-reroute per-prefix enable prefix-priority high
network 192.0.2.1 255.255.255.0 area 0
route-map OSPF-PREFIX-PRIORITY permit 10
match tag 866
```

Example Configuring Repair-Path Selection Policy

The following example shows how to configure a repair-path selection policy that sets SRLG, line card failure and downstream as tiebreaking attributes, and sets their priority indexes:

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute per-prefix tie-break srlg required index 10
  fast-reroute per-prefix tie-break linecard-disjoint index 15
  fast-reroute per-prefix tie-break downstream index 20
  network 192.0.2.1 255.255.255.0 area 0
```

Example Auditing Repair-Path Selection

The following example shows how to keep a record of repair-path selection:

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute keep-all-paths
  network 192.0.2.1 255.255.255.0 area 0
```

Example Prohibiting an Interface from Being a Protecting Interface

The following example shows how to prohibit an interface from being a protecting interface:

```
Router(config)# interface GigabitEthernet 0/0/0
  ip addres
s 192.0.2.1 255.255.255.0
  ip ospf fast-reroute per-prefix candidate disable
```

Additional References

The following sections provide references related to the OSPF RFC 3623 Graceful Restart feature.

Related Documents

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

Related Topic	Document Title
OSPF configuration	Configuring OSPF
Cisco nonstop forwarding	Cisco Nonstop Forwarding
OSPFv3 Graceful Restart	'*OSPFv3 Graceful Restart*' module

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
RFC 2328	*OSPF Version 2*
RFC 3623	*Graceful OSPF Restart*

Technical Assistance

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

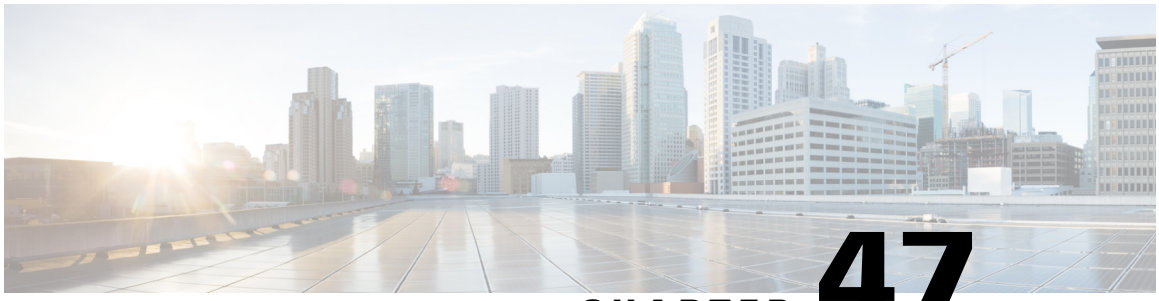
Feature Information for OSPFv2 Loop-Free Alternate Fast Reroute

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 52: Feature Information for OSPFv2 Loop-Free Alternate Fast Reroute

Feature Name	Releases	Feature Information
OSPFv2 Loop-Free Alternate Fast Reroute	Cisco IOS XE Release 3.4S	This feature uses a precomputed alternate next hop to reduce failure reaction time when the primary next hop fails. The following commands were introduced or modified: **debug ip ospf fast-reroute, fast-reroute keep-all-paths, fast-reroute per-prefix (OSPF), fast-reroute tie-break (OSPF), ip ospf fast-reroute per-prefix, prefix-priority, show ip ospf fast-reroute**, **show ip ospf interface**, **show ip ospf neighbor**, **show ip ospf rib .**



CHAPTER 47

OSPFv3 MIB

The OSPFv3 MIB feature enables remote monitoring and troubleshooting of Open Shortest Path First version 3 (OSPFv3) processes using standard Simple Network Management Protocol (SNMP) management workstations. The protocol information collected by the OSPFv3 MIB objects and trap objects can be used to derive statistics that helps monitor and improve overall network performance.

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.

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 OSPFv3 MIB

- Ensure that Open Shortest Path First version 3 (OSPFv3) is configured on the device.
- Ensure that Simple Network Management Protocol (SNMP) is enabled on the device before notifications (traps) can be configured or before SNMP GET operations can be performed.

Restrictions for OSPFv3 MIB Support

- To monitor multiple Open Shortest Path First version 3 (OSPFv3) processes, each process must be associated with a Simple Network Management Protocol (SNMP) context.
- To monitor multiple VRFs, each VRF must be associated with an SNMP context.

Information About OSPFv3 MIB

OSPFv3 MIB

Open Shortest Path First version 3 (OSPFv3) is the IPv6 implementation of OSPF. The OSPFv3 MIB is documented in RFC 5643 and defines a MIB for managing OSPFv3 processes through Simple Network Management Protocol (SNMP).

Users can constantly monitor the changing state of an OSPF network by using MIB objects. The MIB objects gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes.

OSPFv3 TRAP MIB

The ospfv3Notifications MIB object contains the OSPFv3 trap MIB objects that enable and disable OSPF traps in the Cisco IOS CLI. These OSPFv3 trap MIB objects are provided by the RFC 5643 standard OSPFv3 MIB.

How to Configure OSPFv3 MIB

Enabling Specific OSPFv3 Traps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. **snmp-server enable traps ospfv3 errors** [**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**]
5. **snmp-server enable traps ospfv3 rate-limit** *seconds trap-number*
6. **snmp-server enable traps ospfv3 state-change** [**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**]
7. **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	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Device(config)# snmp-server host 172.20.2.162 version 2c public ospfv3`	Specifies a recipient (target host) for Simple Network Management Protocol (SNMP) notification operations. • If the *notification-type* is not specified, all enabled notifications (traps or informs) are sent to the specified host. • If you want to send only the Open Shortest Path First version 3 (OSPFv3) notifications to the specified host, you can use the optional **ospfv3** keyword as the *notification-types* . Entering the **ospfv3** keyword enables the ospfv3Notifications MIB object.
Step 4	**snmp-server enable traps ospfv3 errors** [**bad-packet**] [**config-error**] [**virt-bad-packet**] [**virt-config-error**] **Example:** `Device(config)# snmp-server enable traps ospfv3 errors`	Enables SNMP notifications for OSPFv3 errors.
Step 5	**snmp-server enable traps ospfv3 rate-limit** *seconds trap-number* **Example:** `Device(config)# snmp-server enable traps ospfv3 rate-limit 20 20`	Sets the rate limit for the number of SNMP OSPFv3 notifications that are sent in each OSPFv3 SNMP notification rate-limit window.
Step 6	**snmp-server enable traps ospfv3 state-change** [**if-state-change**] [**neighbor-restart-helper-status-change**] [**neighbor-state-change**] [**nssa-translator-status-change**] [**restart-status-change**] [**virtif-state-change**] [**virtneighbor-restart-helper-status-change**] [**virtneighbor-state-change**]	Enables SNMP OSPFv3 notifications for OSPFv3 transition state changes.

	Command or Action	Purpose
	Example: `Device(config)# snmp-server enable traps ospfv3 state-change`	
Step 7	**end** **Example:** `Device(config)# end`	Exits global configuration mode and enters privileged EXEC mode.

Verifying OSPFv3 MIB Traps on the Device

SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show running-config** [*options*]

Example:

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

Displays the contents of the currently running configuration file and includes information about enabled traps.

- Verifies which traps are enabled.

Configuration Examples for OSPFv3 MIB

Example: Enabling and Verifying OSPFv3 MIB Traps

The following example shows how to enable all OSPFv3 error traps:

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps ospfv3 errors
Device(config)# end
```

The following example shows how to verify that the traps are enabled:

```
Device> enable
Device# show running-config | include traps

snmp-server enable traps ospfv3 errors
```

Additional References for OSPFv3 MIB

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
OSPF configuration tasks	"Configuring OSPF" module in *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard	Title
RFC 5643	*Management Information Base for OSPFv3*

MIBs

MIB	MIBs Link
OSPFv3-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

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

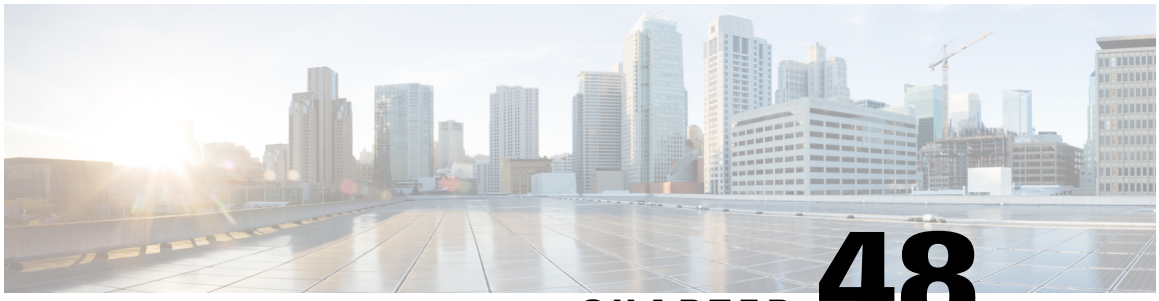
Feature Information for OSPFv3 MIB

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 53: Feature Information for OSPFv3 MIB

Feature Name	Releases	Feature Information
OSPFv3 MIB	Cisco IOS XE Release 3.7S	The OSPFv3 MIB feature enables remote monitoring and troubleshooting of OSPFv3 processes using standard SNMP management workstations. The following commands were introduced or modified: **snmp-server host**, **snmp-server enable traps ospfv3 errors**, **snmp-server enable traps ospfv3 rate-limit**, **snmp-server enable traps ospfv3 state-change**.



CHAPTER 48

Prefix Suppression Support for OSPFv3

This feature enables Open Shortest Path First version 3 (OSPFv3) to hide the IPv4 and IPv6 prefixes of connected networks from link-state advertisements (LSAs). When OSPFv3 is deployed in large networks, limiting the number of IPv4 and IPv6 prefixes that are carried in the OSPFv3 LSAs can speed up OSPFv3 convergence.

This feature can also be utilized to enhance the security of an OSPFv3 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.

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 Prefix Suppression Support for OSPFv3

Before you can use the mechanism to exclude IPv4 and IPv6 prefixes from LSAs, the OSPFv3 routing protocol must be configured.

Information About Prefix Suppression Support for OSPFv3

OSPFv3 Prefix Suppression Support

The OSPFv3 Prefix Suppression Support feature allows you to hide IPv4 and IPv6 prefixes that are configured on interfaces running OSPFv3.

In OSPFv3, addressing semantics have been removed from the OSPF protocol packets and the main LSA types, leaving a network-protocol-independent core. This means that Router-LSAs and network-LSAs no longer contain network addresses, but simply express topology information. The process of hiding prefixes is simpler in OSPFv3 and suppressed prefixes are simply removed from the intra-area-prefix-LSA. Prefixes are also propagated in OSPFv3 via link LSAs

The OSPFv3 Prefix Suppression feature provides a number of benefits.The exclusion of certain prefixes from adverstisements means that there is more memory available for LSA storage, bandwidth and buffers for LSA flooding, and CPU cycles for origination and flooding of LSAs and for SPF computation. Prefixes are also filtered from link LSAs. A device only filters locally configured prefixes, not prefixes learnt via link LSAs. In addition, security has been improved by reducing the possiblity of remote attack with the hiding of transit-only networks.

Globally Suppress IPv4 and IPv6 Prefix Advertisements by Configuring the OSPFv3 Process

You can reduce OSPFv3 convergence time by configuring the OSPFv3 process on a device to prevent the advertisement of all IPv4 and IPv6 prefixes by using the **prefix-suppression** command in router configuration mode or address-family configuration mode.

Note Prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces are not suppressed by the **router mode** or the **address-family** configuration commands because typical network designs require prefixes to remain reachable.

Suppress IPv4 and IPv6 Prefix Advertisements on a Per-Interface Basis

You can explicitly configure an OSPFv3 interface not to advertise its IP network to its neighbors by using the **ipv6 ospf prefix-suppression** command or the **ospfv3 prefix-suppression** command in interface configuration mode.

Note If you have globally suppressed IPv4 and IPv6 prefixes from connected IP networks by configuring the **prefix-suppression** router configuration command, the interface configuration command takes precedence over the router configuration command.

How to Configure Prefix Suppression Support for OSPFv3

Configuring Prefix Suppression Support of the OSPFv3 Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id* [**vrf** *vpn-name*]
4. **prefix-suppression**
5. **end**
6. **show ospfv3**

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* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospfv3 23`	Configures an OSPFv3 routing process and enters router configuration mode.
Step 4	**prefix-suppression** **Example:** `Device(config-router)# prefix-suppression`	Prevents OSPFv3 from advertising all IPv4 and IPv6 prefixes, except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces.
Step 5	**end** **Example:** `Device(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ospfv3**	Displays general information about OSPFv3 routing processes.

	Command or Action	Purpose
	Example: `Device# show ospfv3`	**Note** Use this command to verify that IPv4 and IPv6 prefix suppression has been enabled.

Configuring Prefix Suppression Support of the OSPFv3 Process in Address-Family Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id* [**vrf** *vpn-name*]
4. **address-family ipv6 unicast**
5. **prefix-suppression**
6. **end**
7. **show ospfv3**

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* [**vrf** *vpn-name*] **Example:** `Device(config)# router ospfv3 23`	Configures an OSPFv3 routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**address-family ipv6 unicast** **Example:** `Device(config-router)# address-family ipv6 unicast`	Enters IPv6 address family configuration mode for OSPFv3.
Step 5	**prefix-suppression** **Example:** `Device(config-router-af)# prefix-suppression`	Prevents OSPFv3 from advertising all IPv4 and IPv6 prefixes, except prefixes that are associated with loopbacks, secondary IP addresses, and passive interfaces.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Returns to privileged EXEC mode.
Step 7	**show ospfv3** **Example:** `Device# show ospfv3`	Displays general information about OSPFv3 routing processes. **Note** Use this command to verify that IPv4 and IPv6 prefix suppression has been enabled.

Configuring Prefix Suppression Support on a Per-Interface Basis

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ipv6 ospf prefix-suppression** [**disable**]
   - **ospfv3 prefix-suppression disable**
5. **end**
6. **show ospfv3 interface**

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 0/0`	Configures an interface type and enters interface configuration mode.

Step 4	Do one of the following:
	• **ipv6 ospf prefix-suppression** [**disable**]
	• **ospfv3 prefix-suppression disable**
	
	Example:
	`Device(config-if)# ipv6 ospf prefix-suppression`
	
	Example:
	`Device(config-if)# ospfv3 1 prefix-suppression disable`
		Prevents OSPFv3 from advertising IPv4 and IPv6 prefixes that belong to a specific interface, except those that are associated with secondary IP addresses.
		• When you enter the **ipv6 ospf prefix-suppression** command or the **ospfv3 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:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ospfv3 interface** **Example:** `Device# show ospfv3 interface`	Displays OSPFv3-related interface information. **Note** Use this command to verify that IPv4 and IPv6 prefix suppression has been enabled for a specific interface.

Troubleshooting IPv4 and IPv6 Prefix Suppression

SUMMARY STEPS

1. **enable**
2. **debug ospfv3 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:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ospfv3 lsa-generation** **Example:** `Device# debug ospfv3 lsa-generation`	Displays informations about each OSPFv3 LSA that is generated.
Step 3	**debug condition interface** *interface-type interface-number* [**dlci** *dlci*] [**vc** {*vci* | *vpi* | *vci*}] **Example:** `Device# debug condition interface serial 0/0`	Limits output for some **debug** commands on the basis of the interface or virtual circuit.
Step 4	**show debugging** **Example:** `Device# show debugging`	Displays information about the types of debugging that are enabled for your device.
Step 5	**show logging** [**slot** *slot-number* | **summary**] **Example:** `Device# show logging`	Displays the state of syslog and the contents of the standard system logging buffer.

Configuration Examples for Prefix Suppression Support for OSPFv3

Example: Configuring Prefix Suppression Support for OSPFv3

The following example shows how to configure prefix suppression support for OSPFv3 in router configuration mode:

```
router ospfv3 1
 prefix-suppression
 !
 address-family ipv6 unicast
  router-id 0.0.0.6
  exit-address-family
```

The following example shows how to configure prefix suppression support for OSPFv3 in address-family configuration mode:

```
router ospfv3 1
 !
 address-family ipv6 unicast
  router-id 10.0.0.6
  prefix-suppression
  exit-address-family
```

The following example shows how to configure prefix suppression support for OSPFv3 in interface configuration mode:

```
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
 ipv6 address 2001:201::201/64
 ipv6 enable
 ospfv3 prefix-suppression
 ospfv3 1 ipv4 area 0
 ospfv3 1 ipv6 area 0
 end
```

Additional References for Prefix Suppression Support for OSPFv3

Related Documents

Related Topic	Document Title
Configuring OSPF	“Configuring OSPF”
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Cisco IOS commands	Cisco IOS Master Command List, All Releases

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

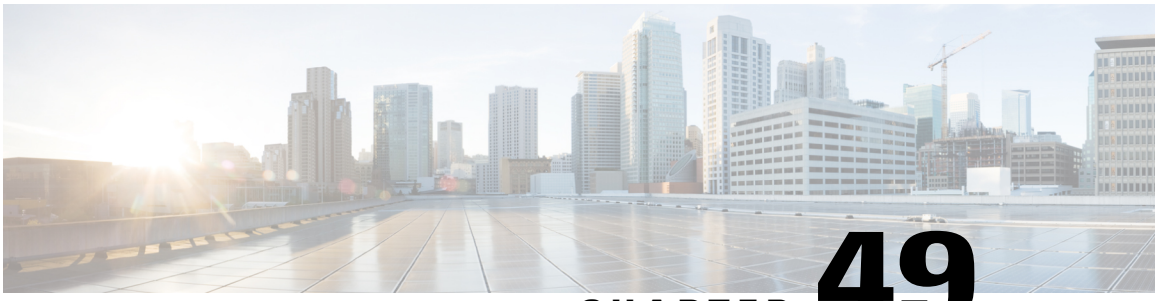
Feature Information for Prefix Suppression Support for OSPFv3

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 54: Feature Information for Prefix Suppression Support for OSPFv3

Feature Name	Releases	Feature Information
Prefix Suppression Support for OSPFv3	Cisco IOS XE Release 3.8S	This feature enables Open Shortest Path First version 3 (OSPFv3) to hide the IPv4 and IPv6 prefixes of connected networks from link-state advertisements (LSAs). This feature can also be used to enhance the security of an OSPFv3 network by allowing the network administrator to prevent IP routing toward internal nodes. The following commands were introduced or modified: • **ipv6 ospf prefix-suppression** • **ospfv3 prefix-suppression** • **prefix-suppression (OSPFv3)**



CHAPTER 49

OSPFv3 VRF-Lite/PE-CE

The OSPFv3 VRF-Lite/PE-CE feature adds Open Shortest Path First version 3 (OSPFv3) support for nondefault VPN routing and forwarding (VRF) instances. OSPFv3 can be used as a provider-edge-customer-edge (PE-CE) routing protocol as specified in RFC 6565, *OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol*. OSPFv3 in a nondefault VRF instance supports routing of IPv4 and IPv6 address families.

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.

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 OSPFv3 VRF-Lite/PE-CE

In Cisco IOS Release 15.2(2)S and later releases, OSPFv3 interface commands in the **ipv6 ospf** format are no longer supported in VRF interface configuration mode. You must configure them in the new format, **ospfv3**.

The **ospfv3** commands can have one of following formats:

- **ospfv3 —**Applies to all OSPFv3 processes and address families on a given interface.

- **ospfv3** *process-id* —Applies to an OSPFv3 process with the configured process ID and to both IPv4 and IPv6 address families.
- **ospfv3** *process-id address-family-ID* —Applies to an OSPFv3 process with the configured process ID and the configured address family.

More specific commands take precedence over less specific commands, as shown in the following descending order:

1. Commands that specify a process ID and an address family.
2. Commands that specify only a process ID.
3. Commands that specify neither a process ID nor an address family.

In Cisco IOS Release 15.2(2)S and later releases, you cannot use the **ipv6 ospf router** *process-id* command to configure OSPFv3 VRF instances. You must configure the **router ospfv3** *process-id* command in global configuration mode and specify the address family for the configured VRF in router configuration mode.

Information About OSPFv3 VRF-Lite/PE-CE

Support for OSPFv3 VRF-Lite and PE-CE

Open Shortest Path First version 3 (OSPFv3) operates in nondefault VPN routing and forwarding (VRF) instances for both IPv6 and IPv4 address families and, transports the routes across a Border Gateway Protocol (BGP) or a Multiprotocol Label Switching (MPLS) backbone. On the provider edge (PE) device, customer routes are installed together by OSPFv3 and BGP in a common VRF or address family and each protocol is configured to redistribute the routes of the other. BGP combines the prefixes redistributed into it with a route-distinguisher value defined for the VRF and advertises them to other MPLS-BGP speakers in the same autonomous system using the VPNv4 or VPNv6 address family as appropriate.

The OSPFv3 route selection algorithm prefers intra-area routes across the back-door link over inter-area routes through the MPLS backbone. Sham-links are a type of virtual link across the MPLS backbone that connect OSPFv3 instances on different PEs. OSPFv3 instances tunnel protocol packets through the backbone and form adjacencies. Because OSPFv3 considers the sham-link as an intra-area connection, sham-link serves as a valid alternative to an intra-area back-door link.

Domain IDs are used to determine whether the routes are internal or external. They describe the administrative domain of the OSPFv3 instance from which the route originates. Every PE has a 48-bit primary domain ID (which may be NULL) and zero or more secondary domain IDs.

How to Configure VRF-Lite/PE-CE

Configuring a VRF in an IPv6 Address Family for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **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	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Configures an OSPF routing process and enters router configuration mode.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters router address family configuration mode.
Step 8	**end** **Example:** `Device(config-router-af)# end`	Exists router address family configuration mode and returns to privileged EXEC mode.

Enabling an OSPFv3 IPv6 Address Family on a VRF Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name* [**downstream** *vrf-name2*]
5. **ipv6 enable**
6. **ospfv3** *process-id* {**ipv4** | **ipv6**} **area** *area-id* [**instance** *instance-id*]
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface Serial6/0`	Specifies an interface type and number and enters interface configuration mode.
Step 4	**vrf forwarding** *vrf-name* [**downstream** *vrf-name2*] **Example:** `Device(config-if)# vrf forwarding v1`	Associates an interface with a VRF.
Step 5	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the interface that is associated with the VRF.
Step 6	**ospfv3** *process-id* {**ipv4** | **ipv6**} **area** *area-id* [**instance** *instance-id*] **Example:** `Device(config-if)# ospfv3 1 ipv6 area 0`	Enables the OSPFv3 IPv6 address family on the VRF interface.
Step 7	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring a Sham-Link for OSPFv3 PE-CE

Before You Begin

The OSPFv3 PE-CE feature supports direct forwarding on Border Gateway Protocol (BGP) routes.

Before you configure a sham-link, you must create a Multiprotocol Label Switching (MPLS) backbone, configure a device as an MPLS VPN PE device, and configure OSPFv3 as the provider-edge-customer-edge (PE-CE) protocol in a virtual routing and forwarding (VRF) instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **description** *string*
5. **vrf forwarding** *vrf-name*
6. **ipv6 address** *ipv6-address/prefix-length*
7. **ipv6 enable**
8. **end**
9. **router ospfv3** *process-id*
10. **address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf** *vrf-name*]
11. **redistribute** *process-id* [*options*]
12. **area** *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**ttl-security hops** *hop-count*]
13. **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	**interface loopback** *interface-number* **Example:** `Device(config)# interface loopback 0`	Creates a loopback interface to be used as an endpoint of the sham-link on a provider edge device and enters interface configuration mode.
Step 4	**description** *string* **Example:** `Device(config-if)# description Sham-link endpoint`	Provides a description of the interface to help you track its status.
Step 5	**vrf forwarding** *vrf-name* **Example:** `Device(config-if)# vrf forwarding vrf1`	Associates the loopback interface with a VRF.

	Command or Action	Purpose
Step 6	**ipv6 address** *ipv6-address/prefix-length* **Example:** `Device(config-if)# ipv6 address 2001:DB8:0:ABCD::1/48`	Configures an IPv6 address of the loopback interface on a provider edge device.
Step 7	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on the loopback interface.
Step 8	**end** **Example:** `Device# end`	Exits interface configuration mode and returns to global configuration mode.
Step 9	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Enters router configuration mode.
Step 10	**address-family** {**ipv4** | **ipv6**} [**unicast** | **multicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrf1`	Enters IPv6 address family configuration mode for OSPFv3.
Step 11	**redistribute** *process-id* [*options*] **Example:** `Device(config-router-af)# redistribute bgp 2`	Redistributes IPv6 routes from the specified source BGP routing domain into the specified destination routing domain. **Note** PE-CE redistribution is always from BGP.
Step 12	**area** *area-id* **sham-link** *source-address destination-address* [**cost** *number*] [**ttl-security hops** *hop-count*] **Example:** `Device(config-router-af)# area 0 sham-link 2001:DB8:0:ABCD::1 2001:DB8:0:ABCD::2 cost 100`	Enables the sham-link and specifies its source and destination addresses.
Step 13	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Configuring a Domain ID for an OSPFv3 PE-CE

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **domain-id type** *type* **value** *hex-value*
9. **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	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Enters router configuration mode.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters address family configuration mode..
Step 8	**domain-id type** *type* **value** *hex-value* **Example:** `Device(config-router-af)# domain-id type 0205 value 800EFFFF12AB`	Configures the BGP domain ID. • The value for **type** can be 0005, 0105, 0205, or 8005. • The value for **value** is an arbitrary 48-bit number encoded as 12 hexadecimal digits.
Step 9	**end** **Example:** `Device(config-router-af)# end`	Exists router address family mode and returns to privileged EXEC mode.

Configuring VRF-Lite Capability for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **router ospfv3** [*process-id*]
7. **address-family ipv6** [**unicast**] [**vrf** *vrf-name*]
8. **capability vrf-lite**
9. **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	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrfsample`	Configures a VRF routing table and enters VRF configuration mode.
Step 4	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 10:1`	Creates routing and forwarding tables for a VRF.
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exists VRF configuration mode and returns to global configuration mode.
Step 6	**router ospfv3** [*process-id*] **Example:** `Device(config)# router ospfv3 2`	Enables router configuration mode for the IPv4 or IPv6 address family.
Step 7	**address-family ipv6** [**unicast**] [**vrf** *vrf-name*] **Example:** `Device(config-router)# address-family ipv6 unicast vrf vrfsample`	Configures an instance of the OSPFv3 process in the VRF routing table for the IPv6 address family and enters address family configuration mode.
Step 8	**capability vrf-lite** **Example:** `Device(config-router-af)# capability vrf-lite`	Applies the multi-VRF capability to the OSPF process.

	Command or Action	Purpose
Step 9	**end** **Example:** `Device(config-router-af)# end`	Exists router address family mode and returns to privileged EXEC mode.

Configuration Examples for OSPFv3 VRF-Lite/PE-CE

Example: Configuring a Provider Edge Device to Provide IPv6 and IPv4 Routing

The following example shows how to configure a provider edge (PE) device to provide IPv6 and IPv4 routing for a user on VRF “v1” and IPv6 routing for a user on VRF “v2”:

```
vrf definition v1
 rd 1:1
 route-target export 100:1
 route-target import 100:1
!
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 route-target export 200:2
 route-target import 200:2
!
address-family ipv6
 exit-address-family
!
interface Loopback1
 vrf forwarding v1
 ipv6 address 2001:DB8:0:ABCD::1/48
!
interface Serial5/0
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:0:ABCD::3/48
 ospfv3 1 ipv6 area 1
!
interface Serial6/0
 vrf forwarding v1
 ip address 10.0.0.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 10.1.1.1
!
router ospfv3
!
log-adjacency-changes detail
!
address-family ipv4 unicast vrf v1
 router-id 10.2.2.2
 redistribute bgp 1
```

```
 exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 2001:DB8:1::1
 domain-id type 0205 value 111111222222
 area 0 sham-link 2001:DB8:0:ABCD::5 2001:DB8:0:ABCD::7
 redistribute bgp 1
 exit-address-family
address-family ipv6 unicast vrf v2
 router-id 2001:DB8:1::3
 redistribute bgp 1
 exit
!
router bgp 1
 bgp router-id 10.3.3.3
 no bgp default ipv4-unicast
 neighbor 10.0.0.4 remote-as 1
 neighbor 10.0.0.4 update-source-Loopback0
!
address-family ipv4
 exit-address-family
!
address-family vpnv4
 neighbor 10.0.0.4
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family vpnv6
 neighbor 10.0.0.4 activate
 neighbor 10.0.0.4 send-community extended
 exit-address-family
!
address-family ipv4 vrf v1
 redistribute ospfv3 1
 exit-address-family
!
address-family ipv6 vrf v1
 redistribute ospf 1
 exit-address-family
!
address-family ipv6 vrf v2
 redistribute ospf 1
 exit-address-family
!
```

Example: Configuring a Provider Edge Device for VRF-Lite

```
vrf definition v1
 rd 1:1
 !
address-family ipv4
 exit-address-family
!
address-family ipv6
 exit-address-family
!
vrf definition v2
 rd 2:2
 !
address-family ipv6
 exit-address-family
!
interface FastEthernet0/0
 no ip address
 !
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 vrf forwarding v1
 ip address 192.168.1.1 255.255.255.0
```

```
 ipv6 enable
 ospfv3 1 ipv6 area 0
 ospfv3 1 ipv4 area 0
!
interface FastEthernet0/0.200
 encapsulation dot1Q 200
 vrf forwarding v2
 ipv6 enable
 ospfv3 1 ipv6 area 0
!
interface FastEthernet0/1
 rf forwarding v1
 ip address 10.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 1 ipv6 area 1
 ospfv3 1 ipv4 area 0
 no keepalive
!
interface FastEthernet0/2
 vrf forwarding v2
 no ip address
 ipv6 address 2001:DB8:1::1
 ipv6 enable
 ospfv3 1 ipv6 area 1
!
router ospfv3 1
!
address-family ipv6 unicast vrf v2
 router-id 192.168.2.1
 capability vrf-lite
 exit-address-family
!
address-family ipv4 unicast vrf v1
  router-id 192.168.1.4
  capability vrf-lite
exit-address-family
!
address-family ipv6 unicast vrf v1
 router-id 192.168.1.1
 capability vrf-lite
 exit-address-family
!
```

Additional References for OSPFv3 VRF-Lite/PE-CE

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference

RFCs

RFC	Title
RFC 5838	Support of Address Families in OSPFv3

RFC	Title
RFC 6565	OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol

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

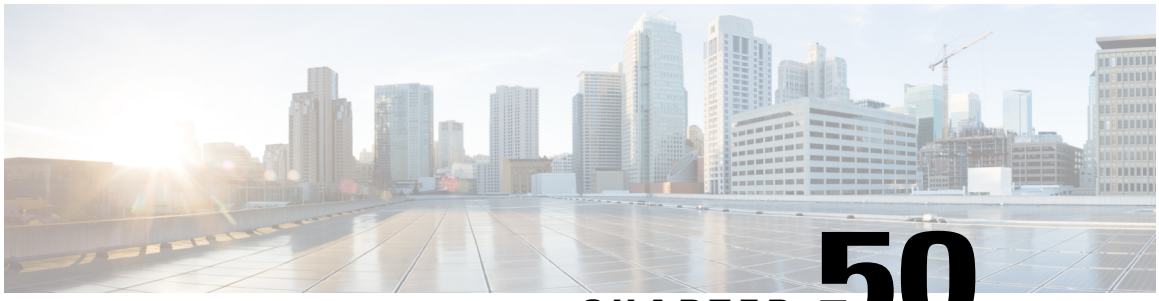
Feature Information for OSPFv3 VRF-Lite/PE-CE

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 55: Feature Information for OSPFv3 VRF-Lite/PE-CE

Feature Name	Releases	Feature Information
OSPFv3 VRF-Lite/PE-CE	Cisco IOS XE Release 3.6S	The OSPFv3 VRF-Lite/PE-CE feature adds OSPFv3 support for nondefault VRF instances. The following commands were introduced or modified: **area sham-link** (OSPFv3), **capability vrf-lite** (OSPFv3).



CHAPTER 50

OSPFv3 ABR Type 3 LSA Filtering

This feature extends the ability of an Area Border Router (ABR) that is running the Open Shortest Path First version 3 (OSPFv3) protocol to filter type 3 link-state advertisements (LSAs) that are sent between different OSPFv3 areas. This feature allows only packets with specified prefixes to be sent from one area to another area and restricts all packets with other prefixes. This type of area filtering can be applied out of a specific OSPFv3 area, into a specific OSPFv3 area, or into and out of the same OSPFv3 areas at the same time.

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.

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.

OSPFv3 ABR Type 3 LSA Filtering

Only type 3 LSAs that originate from an ABR are filtered.

Information About OSPFv3 ABR Type 3 LSA Filtering

Area Filter Support

OSPFv3 area filters allow the filtering of inter-area prefix LSAs on the ABRs. The filter, based on IPv6 prefix lists, can be applied in both directions. In the "in" direction, it filters out the LSAs coming from all other areas when sending the inter-area prefix LSAs into the specified area. In the "out" direction, it filters out the inter-area prefix LSAs generated for the specified area.

The Area Filter Support feature gives the administrator improved control of route distribution between OSPFv3 areas.

How to Configure OSPFv3 ABR Type 3 LSA Filtering

Configuring Area Filter Support for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** *process-id*
4. **area** *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**}
5. **end**
6. **ipv6 prefix-list** *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **permit** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*]

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`	Configures the router to run an OSPFv3 process.
Step 4	**area** *area-id* **filter-list prefix** *prefix-list-name* {**in** | **out**} **Example:** `Device(config-router)# area 1 filter-list prefix test_ipv6 out`	Configures the router to filter interarea routes out of the specified area.
Step 5	**end** **Example:** `Device(config-router)# end`	Returns to global configuration mode.
Step 6	**ipv6 prefix-list** *list-name* [**seq** *seq-number*] {**deny** *ipv6-prefix*/*prefix-length* | **permit** *ipv6-prefix*/*prefix-length* | **description** *text*} [**ge** *ge-value*] [**le** *le-value*] **Example:** `Device(config)# ipv6 prefix-list test_ipv6 seq 5 permit 2011::1/128`	Creates a prefix list with the name specified for the *list-name* argument.

Configuration Examples for OSPFv3 ABR Type 3 LSA Filtering

Example: Area Filter Support for OSPFv3

The following example shows how to configure Area Filter Support for OSPFv3:

```
router ospfv3 1
!
address-family ipv4 unicast
 area 2 filter-list prefix test_ipv4 in
exit-address-family
!
address-family ipv6 unicast
 area 2 filter-list prefix test_ipv6 in
exit-address-family
!
ip prefix-list test_ipv4 seq 5 permit 2.2.2.2/32
!
!
ipv6 prefix-list test_ipv6 seq 5 deny 2011::1/128
```

Additional References for OSPFv3 ABR Type 3 LSA Filtering

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.	—

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

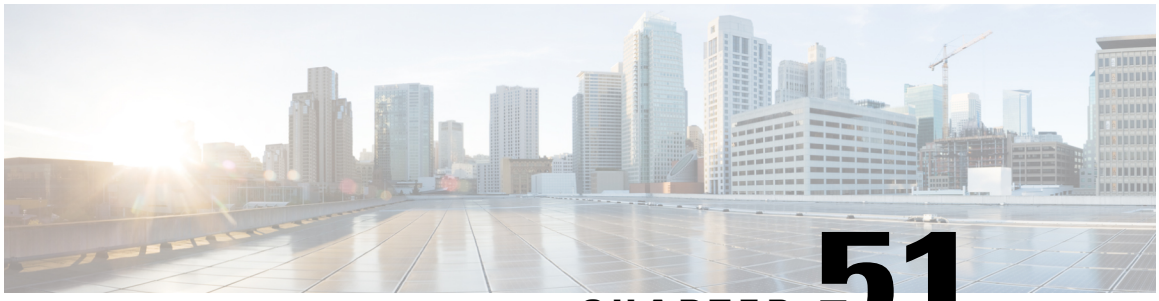
Feature Information for OSPFv3 ABR Type 3 LSA Filtering

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 56: Feature Information for OSPFv3 ABR Type 3 LSA Filtering

Feature Name	Releases	Feature Information
OSPFv3 ABR Type 3 LSA Filtering	Cisco IOS XE Release 3.8 15.3(1)S 15.2(1)E	The OSPFv3 ABR Type 3 LSA Filtering feature extends the ability of an ABR that is running the OSPFv3 protocol to filter type 3 LSAs that are sent between different OSPFv3 areas. This feature allows only packets with specified prefixes to be sent from one area to another area and restricts all packets with other prefixes. This type of area filtering can be applied out of a specific OSPFv3 area, into a specific OSPFv3 area, or into and out of the same OSPFv3 areas at the same time.



CHAPTER 51

OSPFv3 Demand Circuit Ignore

This feature enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** 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.

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 OSPFv3 Demand Circuit Ignore

Demand Circuit Ignore Support

Demand Circuit Ignore Support enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** command. Demand circuit ignore instructs the router not to accept Demand Circuit (DC) negotiation and is a useful configuration option on the point-to-multipoint interface of the Hub router.

How to Configure OSPFv3 Demand Circuit Ignore

Configuring Demand Circuit Ignore Support for OSPFv3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Enter one of the following commands:
   - **ipv6 ospf demand-circuit ignore**
   - **ospfv3 demand-circuit ignore**
5. **end**
6. **show ospfv3** *process-id* [*area-id*] [*address-family*] **[vrf** {*vrf-name* |***** }] **interface** [*type number*] [**brief**]

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 GigabitEthernet 0/1/0`	Configures an interface type and number and enters interface configuration mode.
Step 4	Enter one of the following commands: • **ipv6 ospf demand-circuit ignore** • **ospfv3 demand-circuit ignore**	Prevents an interface from accepting demand-circuit requests from other devices.

	Command or Action	Purpose

	Example:
	`Device(config-if)# ipv6 ospf demand-circuit ignore`
	Example:
	`Device(config-if)# ospfv3 demand-circuit ignore`	

Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ospfv3** *process-id* [*area-id*] [*address-family*] **[vrf** {*vrf-name* **|*** }] **interface** [*type number*] [**brief**] **Example:** `Device# show ospfv3 interface GigabitEthernet 0/1/0`	(Optional) Displays OSPFv3-related interface information.

Configuration Examples for OSPFv3 Demand Circuit Ignore

Example: Demand Circuit Ignore Support for OSPFv3

The following example shows how to configure demand circuit ignore support for OSPFv3:

```
interface Serial0/0
 ip address 6.1.1.1 255.255.255.0
 ipv6 enable
 ospfv3 network point-to-multipoint
 ospfv3 demand-circuit ignore
 ospfv3 1 ipv6 area 0
```

Additional References for OSPFv3 Demand Circuit Ignore

The following sections provide references related to the OSPFv3 Demand Circuit Ignore feature.

Related Documents

Related Topic	Document Title
OSPF configuration tasks	“Configuring OSPF”

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Cisco IOS commands	Cisco IOS Master Command List, All Releases

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

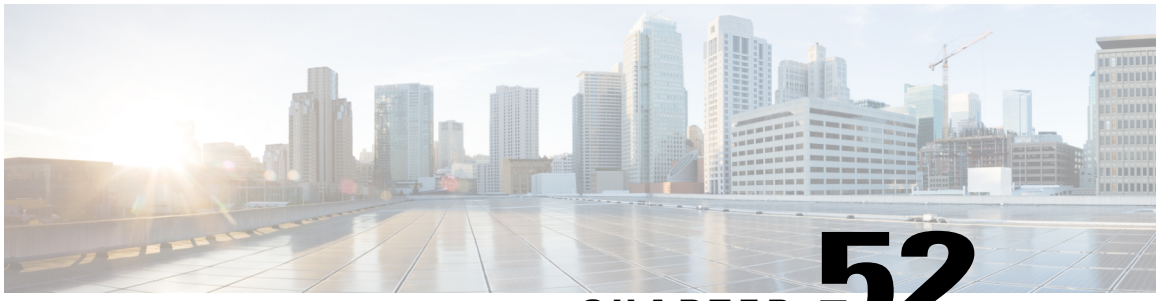
Feature Information for OSPFv3 Demand Circuit Ignore

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 57: Feature Information for OSPFv3 Demand Circuit Ignore

Feature Name	Releases	Feature Information
OSPFv3 Demand Circuit Ignore	Cisco IOS XE Release 3.8	The OSPFv3 Demand Circuit Ignore feature enables you to prevent an interface from accepting demand-circuit requests from other devices by specifying the ignore keyword in the **ipv6 ospf demand-circuit** command. The following commands were introduced or modified: • **ipv6 ospf demand-circuit** • **ospfv3 demand-circuit**



CHAPTER 52

OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

OSPF IPv4 remote loop-free alternate (LFA) IP fast reroute (IPFRR) uses a backup route, precomputed using the dynamic routing protocol, whenever a network fails. The backup routes (repair paths) are pre-computed and installed in the router as the backup for the primary paths. Once the router detects a link or adjacent node failure, it switches to the backup path to avoid traffic loss.

OSPF IPv4 remote LFA IPFRR allows the backup path to be more than one hop away. This feature is particularly useful in some topologies (such as the commonly used ring topology) where an LFA does not have to be directly connected to the protecting router.

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.

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 IPv4 Remote Loop-Free Alternate IP Fast Reroute

- Before performing the tasks in this module, you should be familiar with the concepts described in the "OSPFv2 Loop-Free Alternate Fast Reroute" module.
- LFA must be enabled.
- Your network must be configured for Multiprotocol Label Switching (MPLS).

Restrictions for OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

- The OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute feature is not supported on devices that are virtual links headends.
- The feature is supported only in global VPN routing and forwarding (VRF) OSPF instances.
- The only supported tunneling method is MPLS.
- You cannot configure a traffic engineering (TE) tunnel interface as a protected interface. Use the MPLS Traffic Engineering—Fast Reroute Link and Node Protection feature to protect these tunnels. For more information, see the "MPLS Traffic Engineering—Fast Reroute Link and Node Protection" section in the *Multiprotocol Label Switching Configuration Guide*.
- You can configure a TE tunnel interface in a repair path, but OSPF will not verify the tunnel's placement; you must ensure that it is not crossing the physical interface that it is intended to protect.
- Not all routes can have repair paths. Multipath primary routes might have repair paths for all, some, or no primary paths, depending on the network topology, the connectivity of the computing router, and the attributes required of repair paths.
- Devices that can be selected as tunnel termination points must have a /32 address advertised in the area in which remote LFA is enabled. This address will be used as a tunnel termination IP. If the device does not advertise a /32 address, it may not be used for remote LFA tunnel termination.
- All devices in the network that can be selected as tunnel termination points must be configured to accept targeted LDP sessions using the **mpls ldp discovery targeted-hello accept** command.

Information About OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

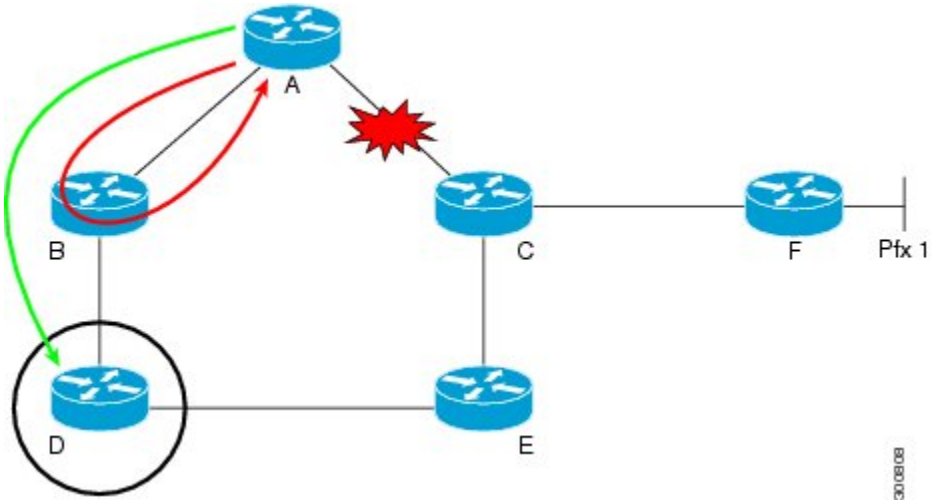
IP Fast Reroute

The IP fast reroute (IPFRR) LFA computation provides protection against link failure. Locally computed repair paths are used to prevent packet loss caused by loops that occur during network reconvergence after a failure. For more information about IPFRR, see RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*.

OSPF IPv4 Remote LFA IPFRR with Ring Topology

Some topologies (for example the commonly used ring-based topology) require protection that is not afforded by LFA FRR alone. Consider the topology shown in the figure below:

Figure 12: Remote LFA IPFRR with Ring Topology



The red looping arrow represents traffic that is looping immediately after a failure between node A and C (before network reconvergence). Device A tries to send traffic destined to F to next-hop B. Device B cannot be used as an LFA for prefixes advertised by nodes C and F. The actual LFA is node D. However, node D is not directly connected to the protecting node A. To protect prefixes advertised by C, node A must tunnel the packet around the failed link A-C to node D, provided that the tunnel does not traverse the failing link.

The OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute feature enables you to tunnel a packet around a failed link to a remote loop-free alternate that is more than one hop away. In the figure above, the green arrow between A and D shows the tunnel that is automatically created by the OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute feature to bypass looping.

Note In the figure above, device A must be configured with **fast-reroute per-prefix remote-lfa tunnel mpls-ldp** to enable remote LFA, and device D must be configured with **mpls ldp discovery targeted-hello accept** to accept targeted LDP sessions.

How to Configure OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Configuring a Remote LFA Tunnel

Perform this task to configure a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix remote-lfa** [**area** *area-id*] **tunnel mpls-ldp**

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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix remote-lfa** [**area** *area-id*] **tunnel mpls-ldp**	Configures a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel via MPLS-LDP.

	Command or Action	Purpose
	Example: `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp`	• Use the **area** *area-id* keyword and argument to specify an area in which to enable LFA FRR.

Configuring the Maximum Distance to a Tunnel Endpoint

Perform this task to configure the maximum distance to the tunnel endpoint in a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix remote-lfa** [**area** *area-id*] **maximum-cost** *distance*

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 ospf** *process-id* **Example:** `Device(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.

	Command or Action	Purpose
Step 4	**fast-reroute per-prefix remote-lfa** [**area** *area-id*] **maximum-cost** *distance* **Example:** `Device(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30`	Configures the maximum distance to the tunnel endpoint in a per-prefix LFA FRR path that redirects traffic to a remote LFA tunnel. • Use the **area** *area-id* keyword and variable to specify an area in which to enable LFA FRR.

Verifying Tunnel Interfaces Created by OSPF IPv4 Remote LFA IPFRR

SUMMARY STEPS

1. **enable**
2. **show ip ospf fast-reroute remote-lfa tunnels**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf fast-reroute remote-lfa tunnels** **Example:** `Device# show ip ospf fast-reroute remote-lfa tunnels`	Displays information about the OSPF per-prefix LFA FRR configuration.

Configuration Examples for OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Example: Configuring a Remote LFA Tunnel

The following example shows how to configure a remote per-prefix LFA FRR in area 2. The remote tunnel type is specified as MPLS-LDP:

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 tunnel mpls-ldp
```

Example: Configuring the Maximum Distance to a Tunnel Endpoint

The following example shows how to set a maximum cost of 30 in area 2:

```
Router(config-router)# fast-reroute per-prefix remote-lfa area 2 maximum-cost 30
```

Example: Verifying Tunnel Interfaces Created by OSPF IPv4 Remote LFA IPFRR

The following example displays information about about tunnel interfaces created by OSPF IPv4 LFA IPFRR:

```
Router# show ip ospf fast-reroute remote-lfa tunnels

      OSPF Router with ID (192.168.1.1) (Process ID 1)
      Area with ID (0)
      Base Topology (MTID 0)

Interface MPLS-Remote-Lfa3
 Tunnel type: MPLS-LDP
 Tailend router ID: 192.168.3.3
 Termination IP address: 192.168.3.3
 Outgoing interface: Ethernet0/0
 First hop gateway: 192.168.14.4
 Tunnel metric: 20
 Protects:
  192.168.12.2 Ethernet0/1, total metric 30
```

Additional References

Related Documents

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

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF" in the *IP Routing: OSPF Configuration Guide*.
OSPFv2 loop-free alternate fast reroute	"OSPFv2 Loop-Free Alternate Fast Reroute" in the *IP Routing: OSPF Configuration Guide*

Standards and RFCs

Standard/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

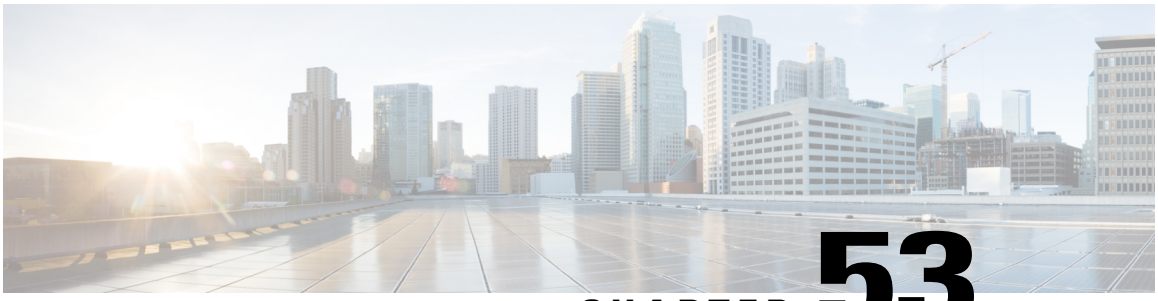
Feature Information for OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

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 58: Feature Information for OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute

Feature Name	Releases	Feature Information
OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute	15.2(2)S Cisco IOS XE Release 3.11S	The OSPF IPv4 Remote Loop-Free Alternate IP Fast Reroute feature enables a backup repair path in the event of node failure, even if the path is multiple hops away. The following commands were introduced or modified: **fast-reroute per-prefix remote-lfa maximum-cost**, **fast-reroute per-prefix remote-lfa tunnel**, and **show ip ospf fast-reroute**.



CHAPTER 53

OSPFv3 Multiarea Adjacency

The OSPFv3 Multiarea Adjacency feature allows you to configure a link that multiple Open Shortest Path First version 3 (OSPFv3) areas can share to enable optimized routing. You can add more than one area to an existing OSPFv3 primary interface.

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.

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 OSPFv3 Multiarea Adjacency

- Ensure that Open Shortest Path First version 3 (OSPFv3) is configured on the primary interface.
- Ensure that the primary interface type is point-to-point.

Restrictions for OSPFv3 Multiarea Adjacency

- A multiarea interface operates only if OSPFv3 is configured on the primary interface and the OSPFv3 network type of the primary interface is point-to-point.
- A multiarea interface exists as a logical construct over a primary interface for OSPFv3; however, the neighbor state on the primary interface is independent of the multiarea interface.
- A multiarea interface establishes a neighbor relationship with the corresponding multiarea interface on the neighboring device. A mixture of multiarea and primary interfaces is not supported.
- A multiarea interface advertises a point-to-point connection to another device in the device link-state advertisement (LSA) for the corresponding area when the neighbor state is full.
- A multiarea interface inherits all the OSPFv3 parameters (such as, authentication) from the primary interface. You cannot configure the parameters on a multiarea interface; however, you can configure the parameters on the primary interface.

Information About OSPFv3 Multiarea Adjacency

OSPFv3 Multiarea Adjacency Overview

Open Shortest Path First version 3 (OSPFv3) allows a single physical link to be shared by multiple areas. This creates an intra-area path in each of the corresponding areas sharing the same link. All areas have an interface on which you can configure OSPFv3. One of these interfaces is designated as the primary interface and others as secondary interfaces.

The OSPFv3 Multiarea Adjacency feature allows you to configure a link on the primary interface to enable optimized routing in multiple areas. Each multiarea interface is announced as a point-to-point unnumbered link. The multiarea interface exists as a logical construct over an existing primary interface. The neighbor state on the primary interface is independent of the neighbor state of the multiarea interface. The multiarea interface establishes a neighbor relationship with the corresponding multiarea interface on the neighboring device. You can only configure multiarea adjacency on an interface that has two OSPFv3 speakers.

Use the **ospfv3 multi-area** command to configure multiarea adjacency on the primary OSPFv3 interface.

How to Configure OSPFv3 Multiarea Adjacency

Configuring OSPFv3 Multiarea Adjacency

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 enable**
5. **ospfv3 multi-area** *multi-area-id*
6. **ospfv3 multi-area** *multi-area-id* **cost** *interface-cost*
7. **ospfv3** *process-id* **ipv6 area** *area-id*
8. **serial restart-delay** *count*
9. **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	**interface** *type number* **Example:** `Device(config)# interface serial 2/0`	Specifies the interface type and number.
Step 4	**ipv6 enable** **Example:** `Device(config-if)# ipv6 enable`	Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.
Step 5	**ospfv3 multi-area** *multi-area-id* **Example:** `Device(config-if)# ospfv3 multi-area 100`	Configures multiarea adjacency on the interface. • The *multi-area-id* argument identifies the OSPFv3 multiarea. The range is from 0 to 4294967295, or you can use an IP address.

	Command or Action	Purpose
Step 6	**ospfv3 multi-area** *multi-area-id* **cost** *interface-cost* **Example:** `Device(config-if)# ospfv3 multi-area 100 cost 512`	(Optional) Specifies the cost of sending a packet on an OSPFv3 multiarea interface. Use this command to specify the cost only if you want the cost of the multiarea interface to be different than the cost of the primary interface.
Step 7	**ospfv3** *process-id* **ipv6 area** *area-id* **Example:** `Device(config-if)# ospfv3 1 ipv6 area 0`	Configures the OSPFv3 interface. • The *process-id* argument identifies the OSPF process. The range is from 1 to 65535. • The *area-id* argument identifies the OSPF area. The range is from 0 to 4294967295, or you can use an IP address.
Step 8	**serial restart-delay** *count* **Example:** `Device(config-if)# serial restart-delay 0`	Sets the amount of time that the router waits before trying to bring up a serial interface when it goes down. The *count* argument specifies the frequency (in seconds) at which that hardware is reset. The range is from 0 to 900.
Step 9	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Verifying OSPFv3 Multiarea Adjacency

SUMMARY STEPS

1. **enable**
2. **show ospfv3 interface brief**
3. **show ospfv3 multi-area**
4. **show ospfv3 interface**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**show ospfv3 interface brief** **Example:** `Device# show ospfv3 interface brief`	Displays brief information about Open Shortest Path First version 3 (OSPFv3) interfaces.
Step 3	**show ospfv3 multi-area** **Example:** `Device# show ospfv3 multi-area`	Displays information about OSPFv3 multiarea interfaces.
Step 4	**show ospfv3 interface** **Example:** `Device# show ospfv3 interface`	Displays information about OSPFv3 interfaces.

Configuration Examples for OSPFv3 Multiarea Adjacency

Example: OSPFv3 Multiarea Adjacency Configuration

```
Device> enable
Device# configure terminal
Device(config)# interface serial 2/0
Device(config-if)# ipv6 enable
Device(config-if)# ospfv3 multi-area 100
Device(config-if)# ospfv3 multi-area 100 cost 512
Device(config-if)# ospfv3 1 ipv6 area 0
Device(config-if)# serial restart-delay 0
Device(config-if)# end
```

Example: Verifying OSPFv3 Multiarea Adjacency

Sample Output for the show ospfv3 interface brief Command

To display brief information about Open Shortest Path First version 3 (OSPFv3) interfaces, use the **show ospfv3 interface brief** command in privileged EXEC mode.

```
Device# show ospfv3 interface brief

Interface PID Area  AF   Cost  State Nbrs F/C
Se2/0     1   0    ipv6  64    P2P   1/1
MA2 1     1   100  ipv6  512   P2P   1/1
```

Sample Output for the show ospfv3 multi-area Command

To display information about OSPFv3 multiarea interfaces, use the **show ospfv3 multi-area** command in privileged EXEC mode.

```
Device# show ospfv3 multi-area

OSPFV3_MA2 is up, line protocol is up
Primary Interface Serial2/0, Area 100
Interface ID 10
MTU is 1500 bytes
Neighbor Count is 1
```

Sample Output for the show ospfv3 interface Command

To display information about OSPFv3 interfaces, use the **show ospfv3 interface** command in privileged EXEC mode.

```
Device# show ospfv3 interface

Serial2/0 is up, line protocol is up
Link Local Address 2001:DB8:0:ABCD::1, Interface ID 10
Area 0, Process ID 1, Instance ID 0, Router ID 10.0.0.12
Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Graceful restart helper support enabled
Index 1/1/1, 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 10.0.0.22
Suppress hello for 0 neighbor(s)
Multi-area interface Count is 1
OSPFV3_MA2 interface exists in area 100 Neighbor Count is 1
OSPFV3_MA2 is up, line protocol is up
Link Local Address 2001:DB8:0:ABCD::1, Interface ID 10
Area 100, Process ID 1, Instance ID 0, Router ID 10.0.0.12
Network Type POINT_TO_POINT, Cost: 512
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Graceful restart helper support enabled
Index 1/1/2, 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 10.0.0.22
```

Additional References for OSPFv3 Multiarea Adjacency

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference

Technical Assistance

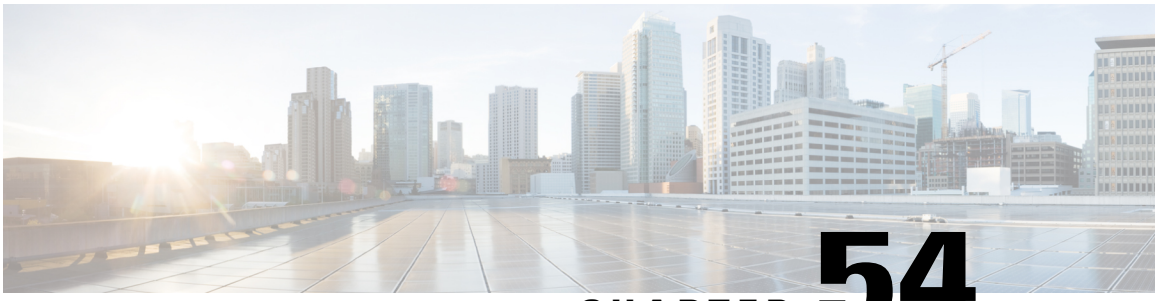
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for OSPFv3 Multiarea Adjacency

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.

Feature Name	Releases	Feature Information
OSPFv3 Multiarea Adjacency		The OSPFv3 Multiarea Adjacency feature allows you to configure a link that multiple Open Shortest Path First version 3 (OSPFv3) areas can share to enable optimized routing. You can add more than one area to an existing OSPFv3 primary interface.



CHAPTER 54

OSPF Limiting Adjacency Formations

The OSPF: Limit Simultaneous Adjacency Formations feature allows you to limit to the number of adjacencies in an OSPF area.

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.

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 Limiting Adjacency Formations

Overview of Limiting Adjacencies

The OSPF: Limit Simultaneous Adjacency Formations feature allows you to limit to the number of adjacencies that are in “exchange” or “loading” state at the same time. A process limit (PL) determines the number of “forming” adjacencies and applies to all adjacencies for the entire process. The term “forming” refers to adjacencies that are in “exchange” or “loading” state. Adjacencies form in an OSPF area during the initial period after the area is created. The Initial Limit applies when no adjacencies have reached the “full” state in an OSPF area. If there are any “full” adjacencies in the area, the new adjacencies are governed by the Process

Limit. At a given point of time, process limit and initial limit are effective in an OSPF area. When there are no adjacencies “forming” in an area, at least one adjacency is allowed to form regardless of the maximum limit specified for it. In other words, the maximum number of adjacencies can be exceeded before adjacencies form in one or more areas. The maximum limit can be exceeded by the number of areas minus one.

When a limit is reached, adjacencies in a state less than EXCHANGE are terminated. To terminate the adjacency, a hello packet is sent to the neighbor which does not have the neighbor’s device ID. This causes the neighbor to put the adjacency in the INIT state. This prevents a deadlock with the neighbor, which could otherwise happen if the neighbor is blocking an adjacency from forming on a different interface. By causing the neighbor to bring the adjacency to INIT, it allows the neighbor to form an adjacency on a different interface. Packets from unknown neighbors are ignored when the limit has been reached or exceeded.

If graceful restart or Cisco nonstop forwarding is configured, the hello packets must be accepted from every neighboring device The restarting device must include the neighbors’ device IDs in its hello packets to prevent the adjacency from being dropped by the neighbor. If graceful restart is in configured, the grace link-state advertisements (LSAs) must be sent in a normal mode and not in a throttling mode. When the device is performing graceful restart and if the limit is reached, new adjacencies are allowed to remain in 2-WAY or EXSTART. However, they are prevented from proceeding to EXCHANGE until the number of forming adjacencies is less than the limit.

Configuring Adjacency Formations

Use the **adjacency stagger** command to configure the maximum limit and the initial limit for an area in the router or address-family configuration modes. The initial limit must not be greater than the process limit. The default value is 300 and the minimum is 1. If the **none** keyword is used, the maximum limit is only effective. The **none** keyword also disables the initial limit for areas. If an initial limit is reached in an area and no adjacencies are forming, no adjacencies will be allowed to form in the area until global number of adjacencies forming is less than the PL.

Use the **ip ospf adjacency stagger disable** or the **ospfv3 adjacency stagger disable** command to disable staggering on an interface. Adjacencies forming on a disabled interface are counted towards throttling limits. Disabling the throttling on an interface allows exceeding the maximum limit when the maximum limit is reached and a new adjacency forms on an interface where throttling is disabled.

Note When using the **no adjacency stagger** command to disable the feature, the command is displayed in the running configuration. To return to the default values, use the **default adjacency stagger** command. After using this command, the **adjacency stagger** command does not appear in the running configuration.

How to Configure OSPF Limiting Adjacency Formations

Configuring Adjacency Formations Globally

Configuring Adjacency Limit in the Router Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **adjacency stagger** {*initial-limit* | **none**} *maximum-limit*
5. **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 ospf** *process-id* **Example:** `Device(config)# router ospf 109`	Enables OSPF routing and enters router configuration mode.
Step 4	**adjacency stagger** {*initial-limit* | **none**} *maximum-limit* **Example:** `Device(config-router)# adjacency stagger 10 50`	Controls the number of adjacencies forming in an area. • *initial-limit*—Minimum number of adjacencies allowed in an area. • *maximum-limit*—Maximum number of adjacencies allowed in an area. • **none**—No minimum number for adjacencies allowed in an area.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring Adjacency Limit in the Address Family Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospfv3** [*process-id*]
4. Do one of the following:
   - **address-family ipv4 unicast**
   - **address-family ipv6 unicast**
5. **adjacency stagger** {*initial-limit* | **none**} {*maximum-limit*| **disable**}
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 OSPFv3 router configuration mode for the IPv4 or IPv6 address family.
Step 4	Do one of the following: • **address-family ipv4 unicast** • **address-family ipv6 unicast**	Enters IPv4 or IPv6 address family configuration mode for OSPFv3.

	Command or Action	Purpose

	Example:
	`Device(config-router)# address-family ipv4 unicast`
	
	Example:
	`Device(config-router)# address-family ipv6 unicast`	

Step 5	**adjacency stagger** {*initial-limit* | **none**} {*maximum-limit*| **disable**} **Example:** `Device(config-router-af)# adjacency stagger 10 50`	Controls the number of adjacencies forming in an area. • *initial-limit*—Minimum number of adjacencies allowed in an area. • **none**—No minimum number for adjacencies allowed in an area. • *maximum-limit*—Maximum number of adjacencies allowed in an area. • **disable**—Disable adjacency formations.
Step 6	**end** **Example:** `Device(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.

Disabling Adjacency Staggering in the Interface Configuration Mode

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip ospf adjacency stagger disable**
   - **ospfv3 adjacency stagger disable**
5. **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	**interface** *type number* **Example:** `Device(config)# interface serial 2/0`	Specifies the interface and enters interface configuration mode.

Step 4	Do one of the following:
	• **ip ospf adjacency stagger disable**
	• **ospfv3 adjacency stagger disable**
	
	Example:
	`Device(config-if)# ip ospf adjacency stagger disable`
	
	Example:
	`Device(config-if)# ospfv3 adjacency stagger disable`
		Disables adjacency staggering on the interface.

Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Verifying Adjacency Staggering

SUMMARY STEPS

1. **enable**
2. **show ip ospf**
3. **show ospfv3**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip ospf**

Example:

```
Device# show ip ospf

 Routing Process "ospf 10" with ID 10.8.3.3
 Start time: 2w0d, Time elapsed: 00:16:43.033
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Supports NSSA (compatible with RFC 3101)
 Supports Database Exchange Summary List Optimization (RFC 5243)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 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
 EXCHANGE/LOADING adjacency limit: initial 300, process maximum 300
 Number of external LSA 0. Checksum Sum 0x000000
 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 0. 0 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
```

Displays information about OSPF routing processes.

Step 3 **show ospfv3**

Example:

```
Device# show ospfv3

 OSPFv3 12 address-family ipv6
 Router ID 10.8.3.3
 Supports NSSA (compatible with RFC 3101)
 Supports Database Exchange Summary List Optimization (RFC 5243)
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 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
 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
 Retransmission limit dc 24 non-dc 24
 EXCHANGE/LOADING adjacency limit: initial 10, process maximum 50
```

```
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 100 mbps
RFC1583 compatibility enabled
```

Displays information about OSPFv3 routing processes.

Configuration Examples for OSPF Limiting Adjacency Formations

Example: Configuring Adjacency Limit in the Router Configuration Mode

```
Device> enable
Device# configure terminal
Device(config)# router ospf 109
Device(config-router)# adjacency stagger 10 50
Device(config-router)# end
```

Example: Configuring Adjacency Limit in the Address Family Configuration Mode

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# adjacency stagger 10 50
Device(config-router-af)# end
```

Example: Disabling Adjacency in the Interface Configuration Mode

```
Device> enable
Device# configure terminal
Device(config)# interface serial 2/0
Device(config-if)# ospfv3 adjacency stagger disable
Device(config-if)# end
```

Additional References for OSPF Limiting Adjacency Formations

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Configuring OSPF	Configuring OSPF

Related Topic	Document Title
Multiarea Adjacency	• OSPFv2 Multiarea Adjacency • OSPFv3 Multiarea Adjacency

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 Limiting Adjacencies Formations

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 59: Feature Information for OSPF Limiting Adjacencies Formations

Feature Name	Releases	Feature Information
OSPF: Limit Simultaneous Adjacency Formations	Cisco IOS XE Release 3.15S	The OSPF: Limit Simultaneous Adjacency Formations feature allows you to limit to the number of adjacencies in an OSPF area. The following commands were introduced or modified: **adjacency stagger**, **ip ospf adjacency stagger disable**, **ip ospfv3 adjacency stagger disable**, **show ip ospf**, **show ip ospfv3**.