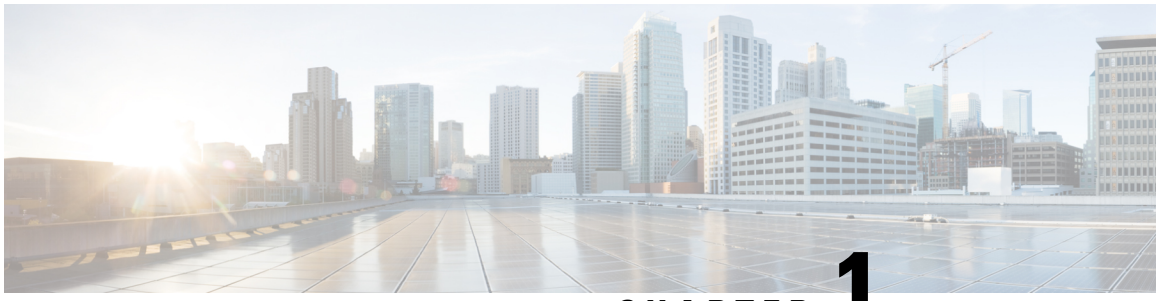
IP Routing: OSPF Configuration Guide for Cisco Catalyst IE3x00 Rugged, IE 3400 Heavy Duty, and ESS3300 Series Switches, Cisco IOS XE 16.12.x

First Published: 2019-08-12

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

CONTENTS



CHAPTER 1

Configuring OSPF

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.

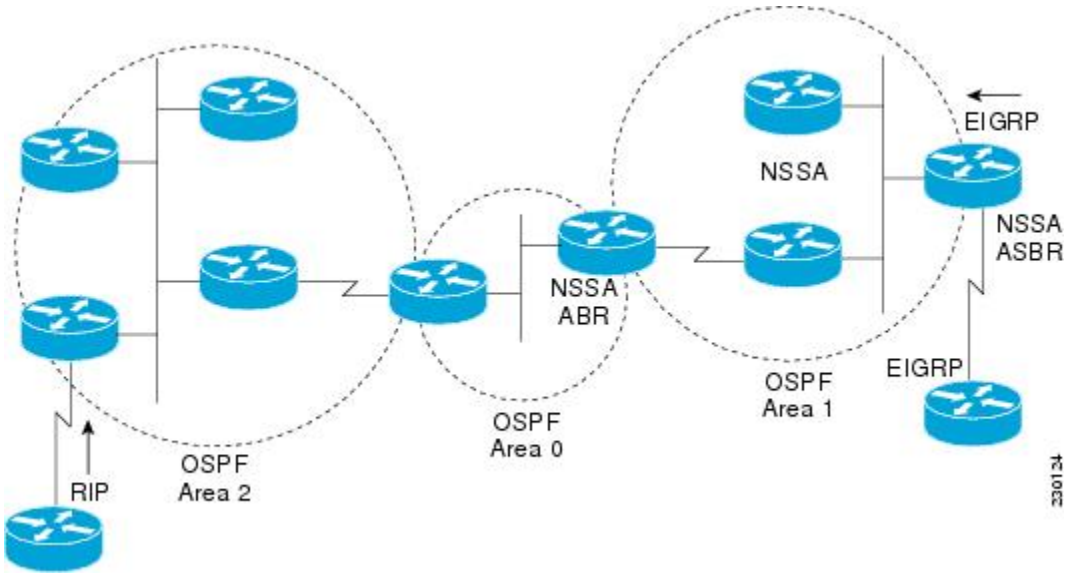
As with OSPF stub areas, NSSA areas cannot be injected with distributed routes via Type 5 LSAs. Route redistribution into an NSSA area is possible only with a special type of LSA that is known as Type 7 that can exist only in an NSSA area. An NSSA ASBR generates the Type 7 LSA so that the routes can 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.

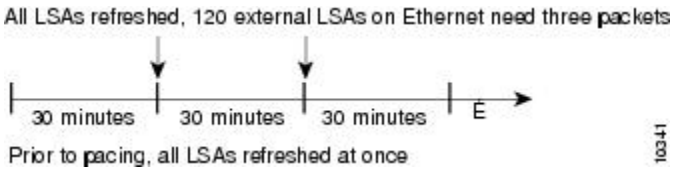
OSPF LSA group pacing is enabled by default. For typical customers, the default group pacing interval for refreshing, checksumming, and aging is appropriate and you need not configure this feature.

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



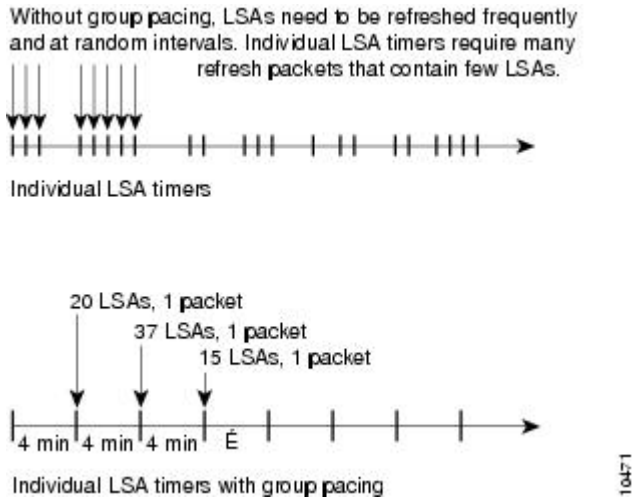
LSA Group Pacing with Multiple Timers

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.
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.

	Command or Action	Purpose
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:**	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface Gigabitethernet 0/0`	
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.
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:**	Specifies the authentication type for an interface.

	Command or Action	Purpose
	`Device(config-if)# ip ospf authentication message-digest`	
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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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 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.
Step 4	**area** *area-id* **authentication** **Example:**	Enables authentication for an OSPF area.

	Command or Action	Purpose
	`Device(config-router)# area 10.0.0.0 authentication`	
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.

	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 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 10.1.0.0 255.255.0.0 not-advertise`	Controls the route summarization and filtering during the translation and limits the summary to NSSA areas.
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.
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:**	Exits router configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-router)# end`	

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.
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*]	Establishes a virtual link.

	Command or Action	Purpose
	Example: `Device(config-router-af)# area 1 virtual-link 10.1.1.1 router1`	

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
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.
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:**	Differentiates high -bandwidth links.

	Command or Action	Purpose
	`Device(config-router)# auto-cost reference-bandwidth 101`	
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.
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:**	Exits router configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-router)# end`	

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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.

Command	Purpose
	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*]	

Command	Purpose
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.
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.

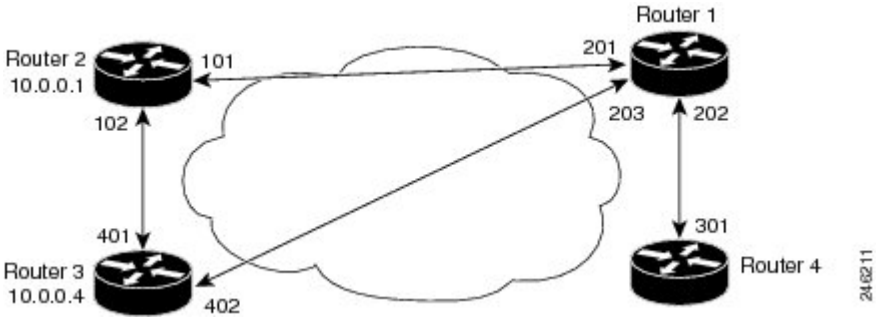
Because the maximum size of an IP packet is 65,535 bytes, there is still an upper bound on the number of links possible on a router.

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.

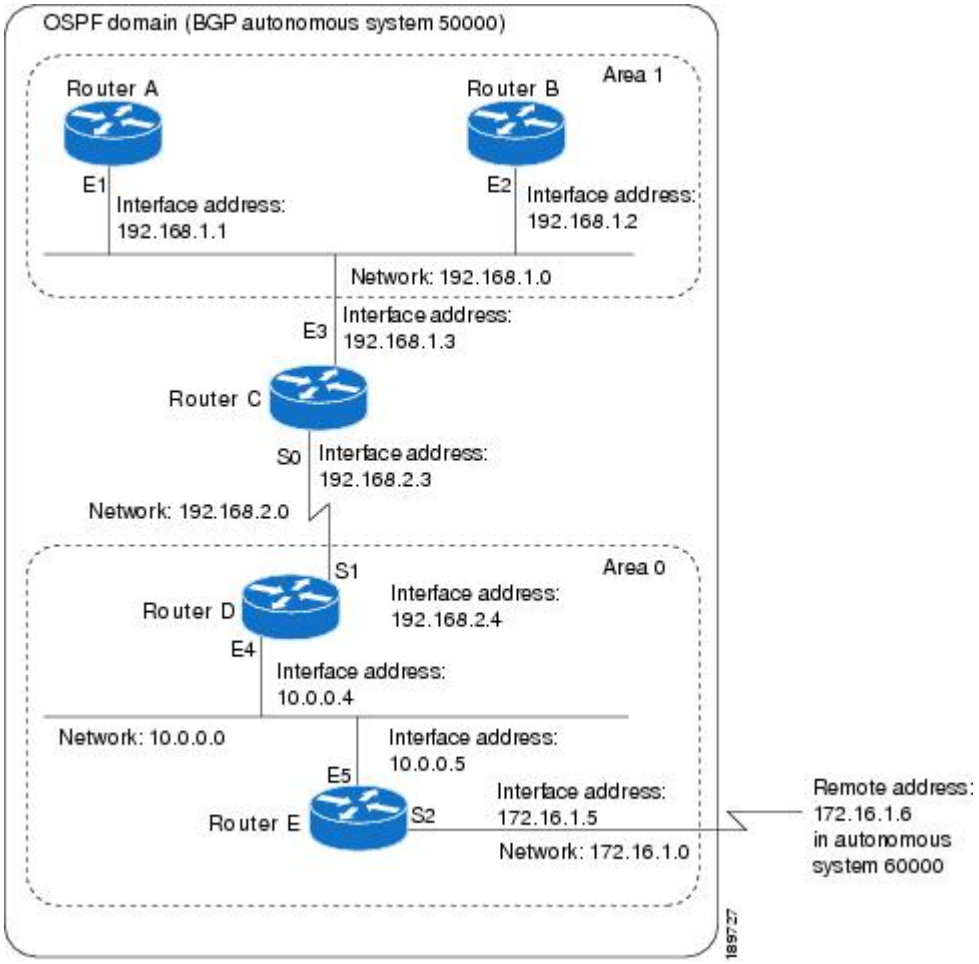
The second **network area** command is evaluated next. For area 2, the same process is then applied to all interfaces (except Ethernet interface 0). Assume that a match is determined for Ethernet interface 1. OSPF is then enabled for that interface, and Ethernet interface 1 is attached to area 2.

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
```

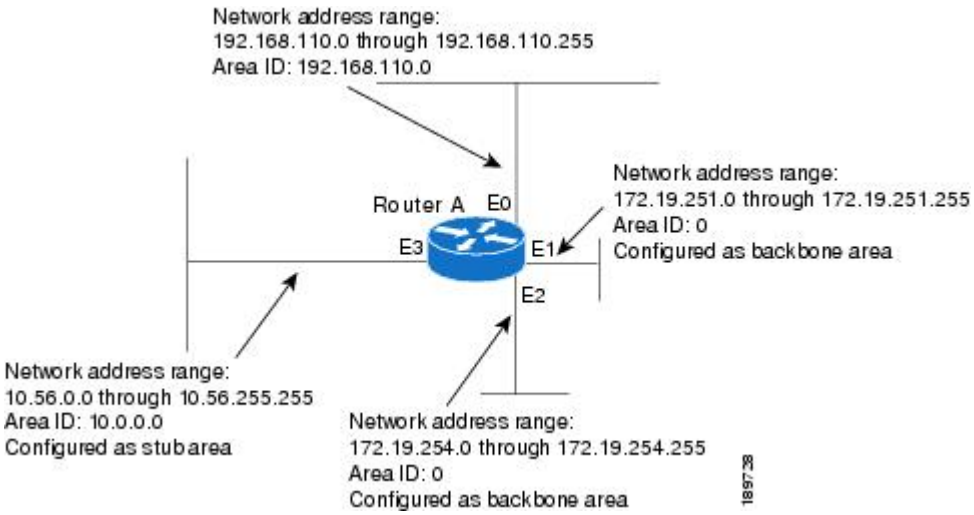
Example: Complex OSPF Configuration for ABR

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.

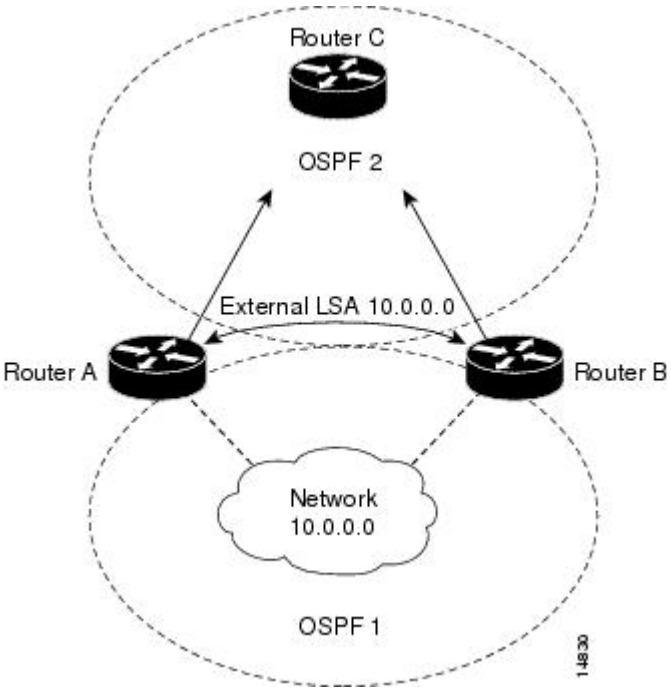
Note Only routes external to the OSPF process can be used for tracking, such as non-OSPF routes or OSPF routes from a separate OSPF process.

```
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

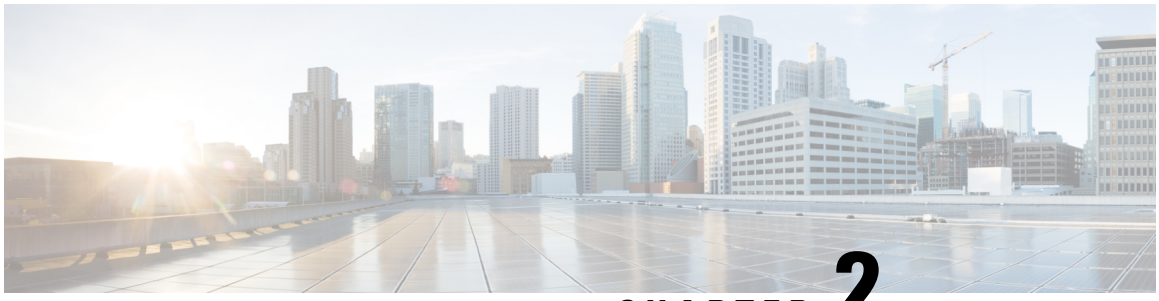
Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Protocol-independent features that work with OSPF	"Configuring IP Routing Protocol-Independent Features" module in *IP Routing: Protocol-Independent Configuration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



CHAPTER 2

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.

Note When key chain has more than one key, OSPF selects the key that has the maximum life time. Key having an infinite lifetime is preferred. If keys have the same lifetime, then key with the higher key ID is preferred.

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.
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.

	Command or Action	Purpose
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** **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 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 3: 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 4: 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.

Field	Description
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

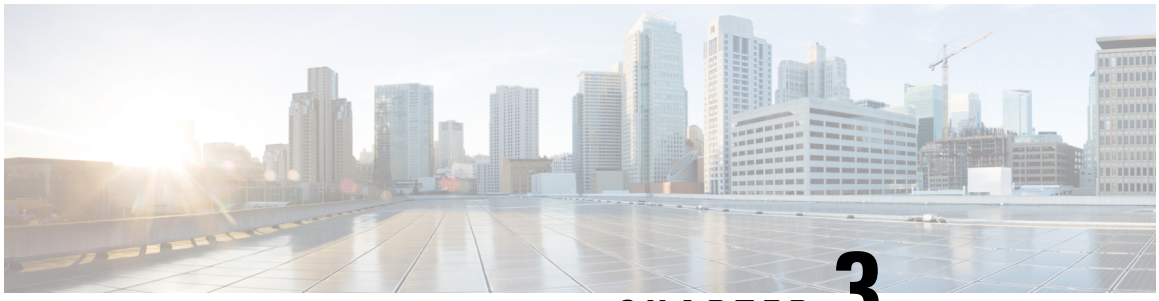
Technical Assistance

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 5: 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 3

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 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.
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

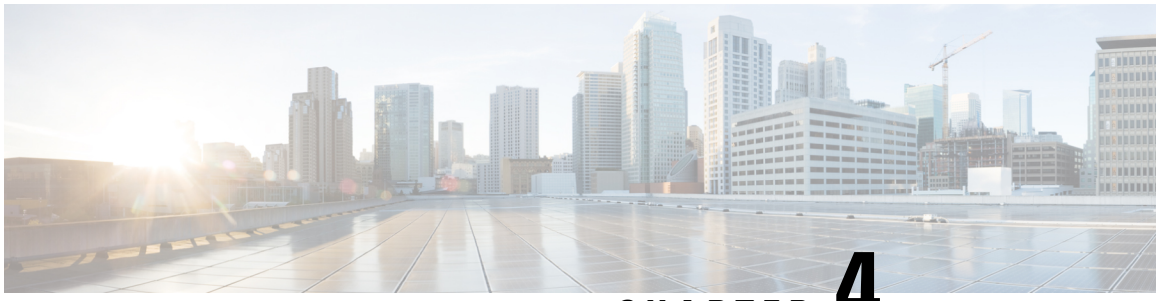
Feature Information for OSPF Stub Router Advertisement

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 6: 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 4

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.

	Command or Action	Purpose
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

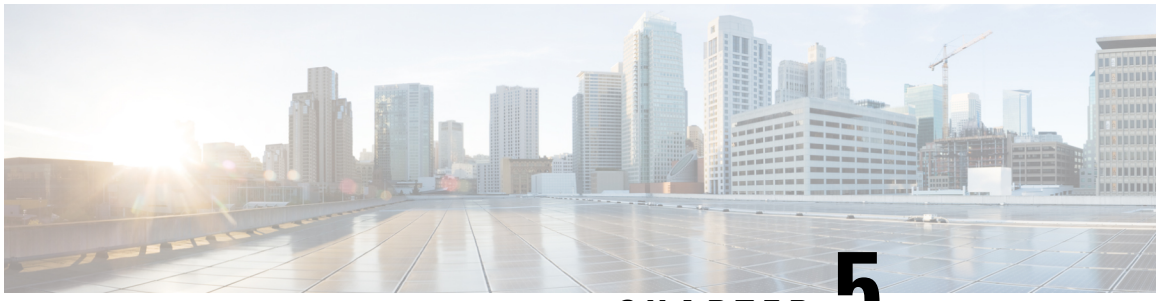
Feature Information for OSPF Update Packet-Pacing Configurable Timers

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 7: 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 5

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. • 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,

	Command or Action	Purpose
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

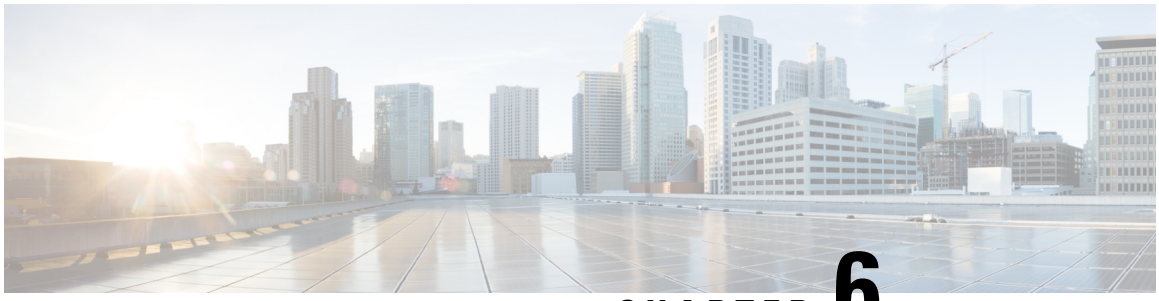
Feature Information for OSPFv2 Multiarea Adjacency

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 8: 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 6

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.
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.
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

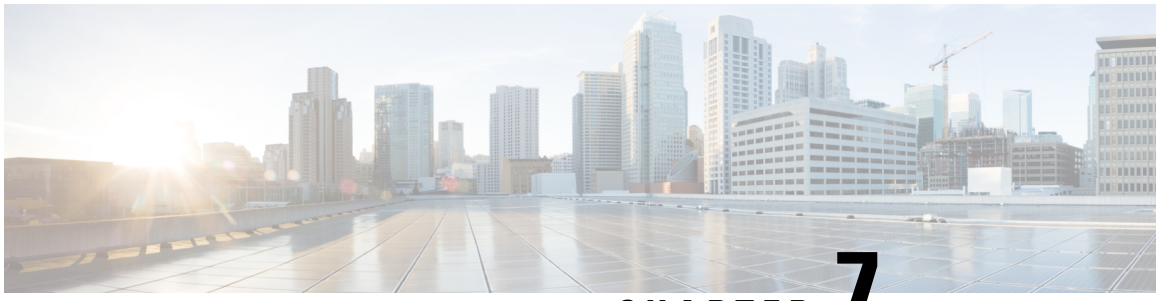
Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, 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 7

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** [**strict-mode**]
7. **default** {**area** *area-ID*[**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*]
8. **ignore lsa mospf**
9. **interface-id snmp-if-index**
10. **log-adjacency-changes** [**detail**]
11. passive-interface [**default** | *interface-type interface-number*]
12. **queue-depth** {**hello** | **update**} {*queue-size* | **unlimited**}
13. router-id {*router-id*}

DETAILED STEPS

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

	Command or Action	Purpose
	`Device(config-router)# area 1`	
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** [**strict-mode**] **Example:** `Device(config-router)# bfd all-interfaces`	Enables BFD for an OSPFv3 routing process **[strict-mode]** - BFD session is established in the strict-mode. In the strict-mode, the OSPF session is not established till the BFD session is established.
Step 7	**default** {**area** *area-ID*[**range** *ipv6-prefix* | **virtual-link** *router-id*]} [**default-information originate** [**always** | **metric** | **metric-type** | **route-map**] | **distance** | **distribute-list** *prefix-list prefix-list-name* {**in** | **out**} [*interface*] | **maximum-paths** *paths* | **redistribute** *protocol* | **summary-prefix** *ipv6-prefix*] **Example:** `Device(config-router)# default area 1`	Returns an OSPFv3 parameter to its default value.
Step 8	**ignore lsa mospf** **Example:** `Device(config-router)# ignore lsa mospf`	Suppresses the sending of syslog messages when the device receives LSA Type 6 multicast OSPFv3 packets, which are unsupported.
Step 9	**interface-id snmp-if-index** **Example:** `Device(config-router)# interface-id snmp-if-index`	Configures OSPFv3 interfaces with Simple Network Management Protocol (SNMP) MIB-II interface Index (ifIndex) identification numbers in IPv4 and IPv6.
Step 10	**log-adjacency-changes** [**detail**] **Example:** `Device(config-router)# log-adjacency-changes`	Configures the 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:**	Configures the number of incoming packets that the IPv4 OSPFv3 process can keep in its queue.

	Command or Action	Purpose
	`Device(config-router)# queue-depth update 1500`	
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.

	Command or Action	Purpose
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* / *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:**	Returns an OSPFv3 parameter to its default value.

	Command or Action	Purpose
	`Router(config-router-af)# default area 1`	
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.
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.
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.

	Command or Action	Purpose
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.
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:** **Example:** or **Example:** **address-family ipv4** **unicast** **Example:** `Router(config-router)# 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:** `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*]	Enables OSPFv3 on an interface with the IPv4 or IPv6 AF. or Enables OSPFv3 on an interface.

	Command or Action	Purpose

	• **ipv6 ospf** *process-id* **area** *area-id* [**instance** *instance-id*]
	Example:
	`Device(config-if)# ospfv3 1 area 1 ipv4`
	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.
Step 2	**configure terminal** **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router# configure terminal`	
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.

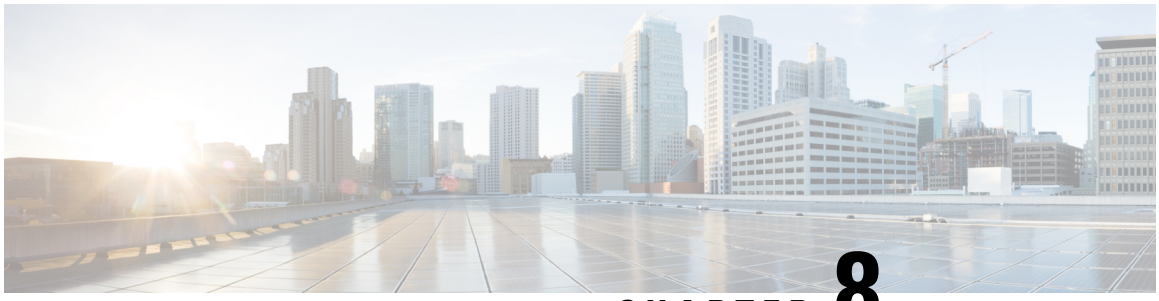
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 9: 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 neighbor**, **show ospfv3 request-list**, **show ospfv3**

Feature Name	Releases	Feature Information
		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 8

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

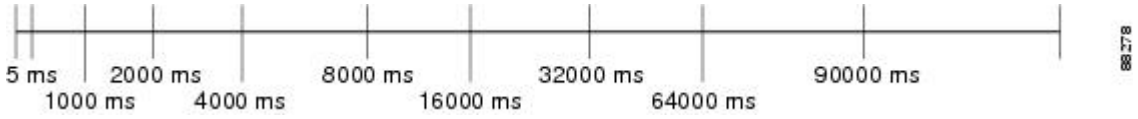
SPF calculations occur at the interval set by the **timers throttle spf**command. The wait interval indicates the amount of time to wait until the next SPF calculation occurs. Each wait interval after that calculation is twice as long as the previous one until the wait interval reaches the maximum wait 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 9: SPF Calculation Intervals Set by the timers throttle spf Command

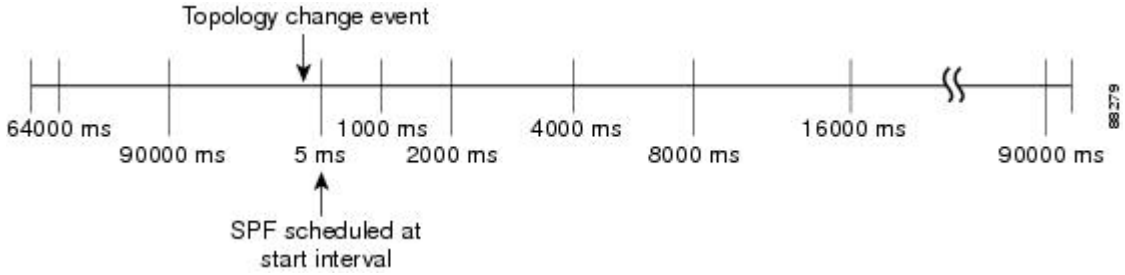


Notice that the wait interval between SPF calculations doubles when at least one topology change event is received during the previous wait interval. Once the maximum wait time is reached, the wait interval remains the same until the topology stabilizes and no event is received in that interval.

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 10: 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

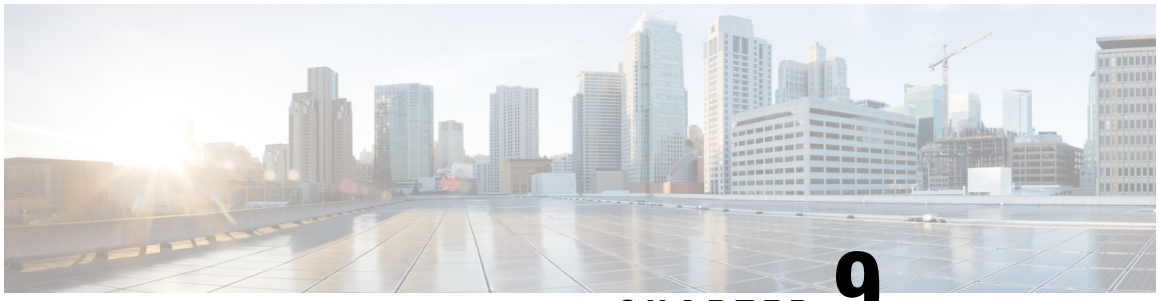
Feature Information for OSPF Shortest Path First Throttling

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 10: 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 9

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.
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:**	Redistributes routes from one routing domain into another routing domain.

	Command or Action	Purpose
	`Router(config-router)# redistribute eigrp 10`	
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:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
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. • 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

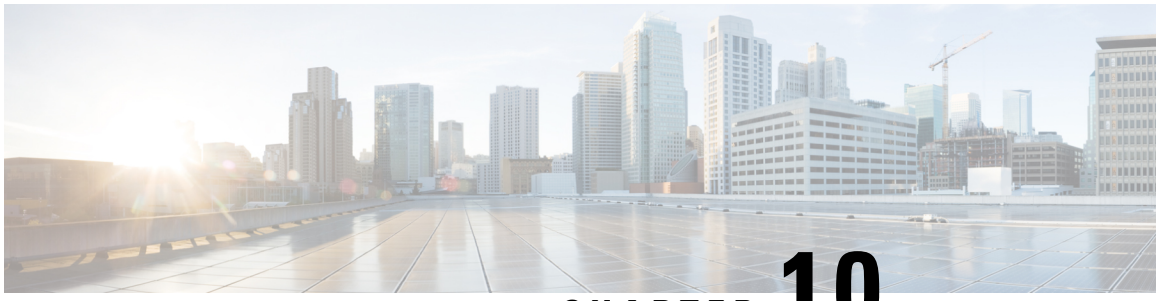
Feature Information for OSPF Limit on Number of Redistributed Routes

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 11: 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 10

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.
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**]	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.

	Command or Action	Purpose
	[**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`	
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

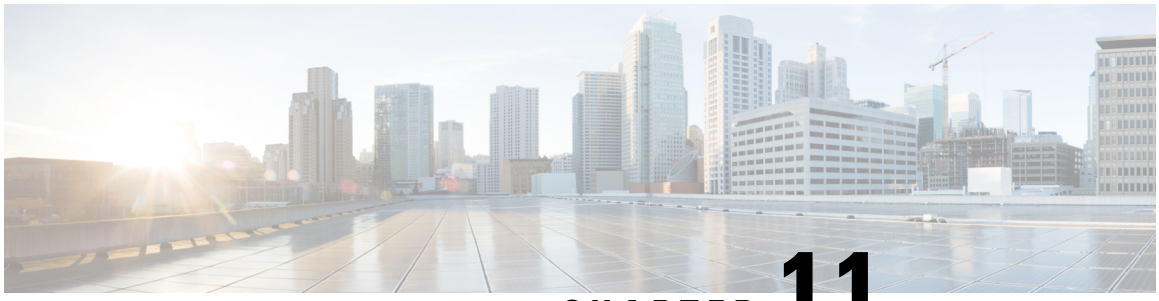
Feature Information for OSPFv3 Max-Metric Router LSA

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 12: 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 11

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**	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 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.

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`
		(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.

	Command or Action	Purpose
	Example: `LSAID: 192.168.4.1 Type: 3 Adv Rtr: 172.17.2.2 Due in: 00:00:00.028`	

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`
	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:
		(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
	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 **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:**	

	Command or Action	Purpose
	SPF algorithm last executed 04:28:18.396 ago **Example:** SPF algorithm executed 8 times **Example:** Area ranges are **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

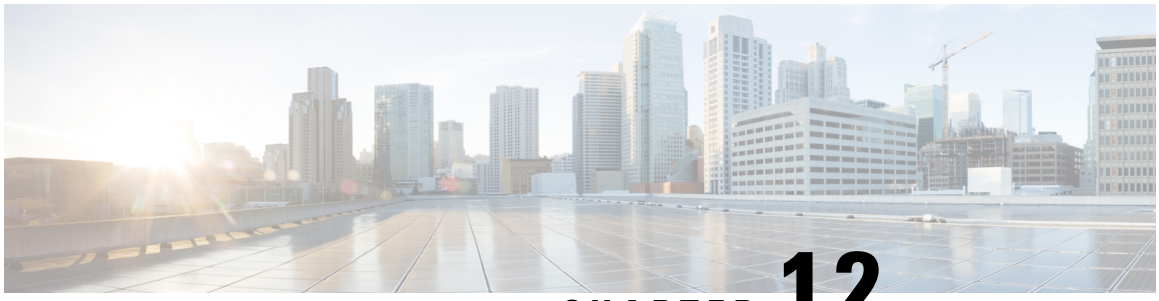
Feature Information for OSPF Link-State Advertisement Throttling

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 13: 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 12

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"

Related Topic	Document Title
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

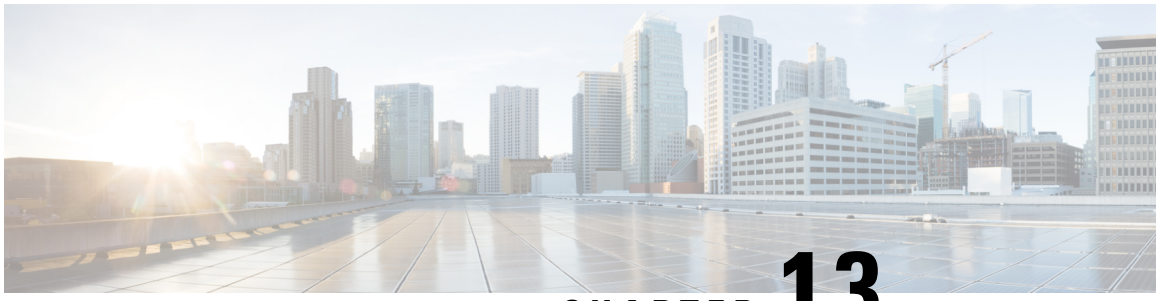
Feature Information for OSPF Area Transit Capability

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 14: 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 13

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.
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.

	Command or Action	Purpose
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

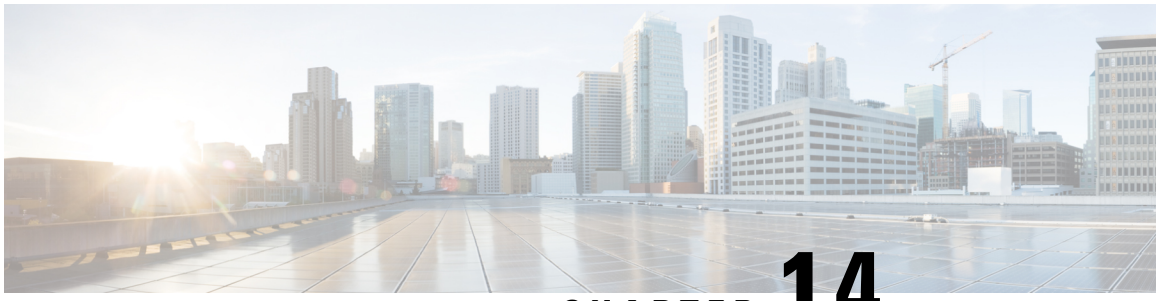
Feature Information for OSPF Link-State Database Overload Protection

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 15: 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 14

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.
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.

	Command or Action	Purpose
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:**	Enables OSPFv3 router configuration mode.

	Command or Action	Purpose
	`Device(config)# ipv6 router ospf 1`	
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.
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*
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

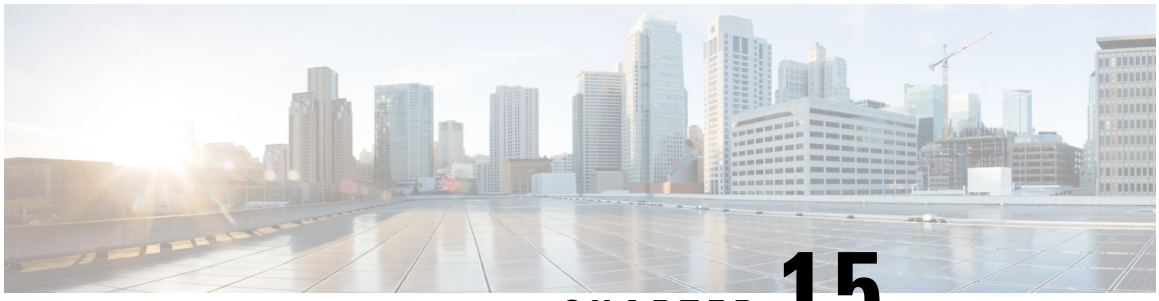
Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

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 16: Feature Information for OSPFv3 Fast Convergence: LSA and SPF Throttling

Feature Name	Releases	Feature Information
OSPFv3 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.



CHAPTER 15

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 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.

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 in Translated Type-5 LSAs

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

Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs

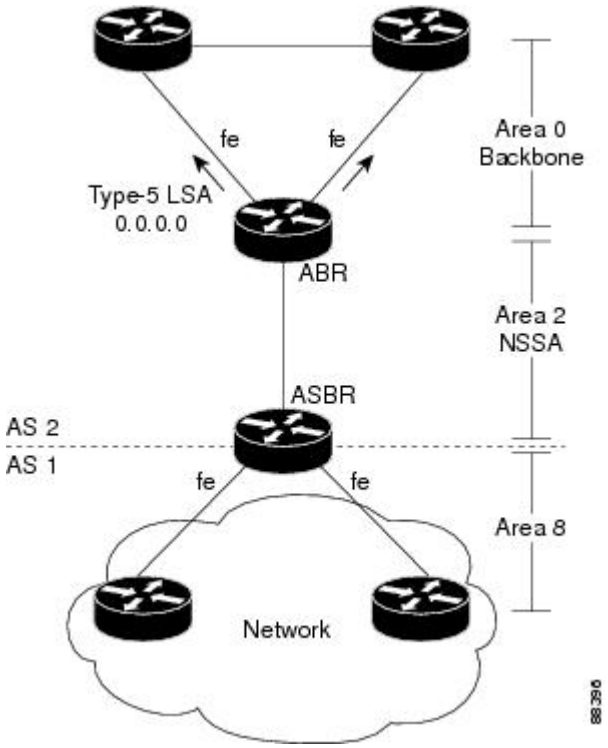
Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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 routers 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 11: 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 router, in this case, the translating NSSA ABR.

Before configuring this feature, consider the following caution.

Caution Configuring this feature causes the router 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 OSPF Forwarding Address in Translated Type-5 LSAs

Suppressing OSPF Forwarding Address in Translated Type-5 LSAs

Caution Configuring this feature causes the router 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.
Step 3	**router ospf** *process-id* **Example:**	Enables OSPF routing and enters device configuration mode. • The *process-id* argument identifies the OSPF process.

	Command or Action	Purpose
	`Device(config)# router ospf 1`	
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 in Translated Type-5 LSAs

Example Suppressing OSPF Forwarding Address in Translated Type-5 LSAs

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

```
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 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

Related Documents

Related Topic	Document Title
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
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

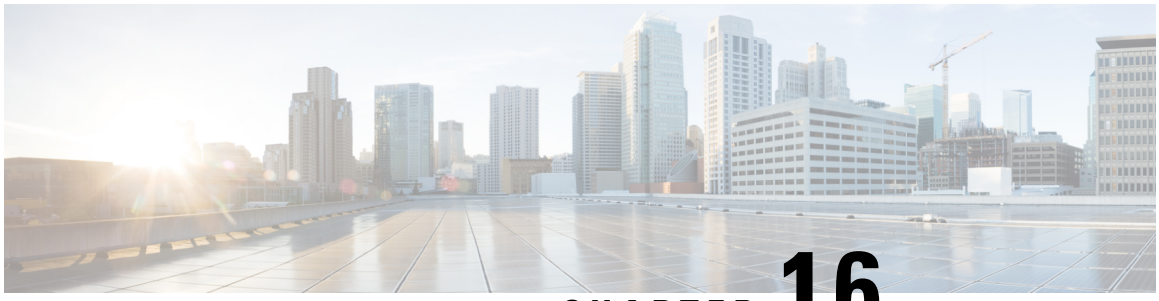
Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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 OSPF Forwarding Address Suppression in Translated Type-5 LSAs

Feature Name	Releases	Feature Information
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 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: • **area nssa translate** • **show ip ospf**



CHAPTER 16

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*] **Example:** `Router(config-if)# no ip directed-broadcast`	Drops directed broadcasts destined for the subnet to which that interface is attached, rather than broadcasting them. • The forwarding of IP directed broadcasts on Ethernet interface 1/0 is disabled.

	Command or Action	Purpose
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

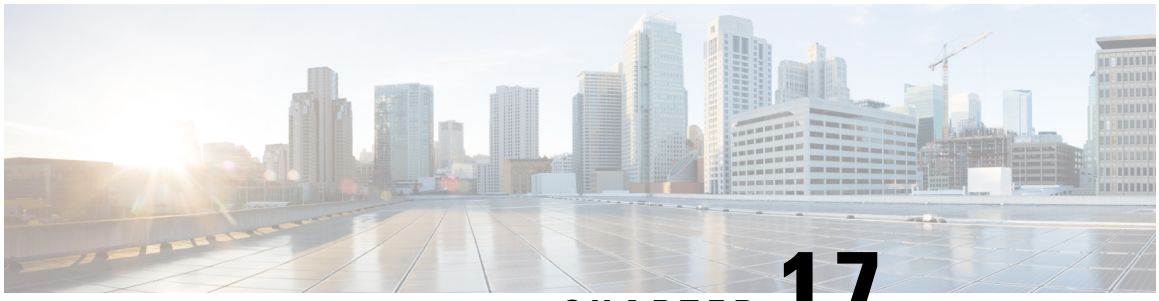
Feature Information for OSPF Per-Interface Link-Local Signaling

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 18: 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 17

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.
Step 3	**router ospfv3** *process-id* **Example:** `Device(config)# router ospfv3 1`	Configures the router to run an OSPFv3 process.

	Command or Action	Purpose
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

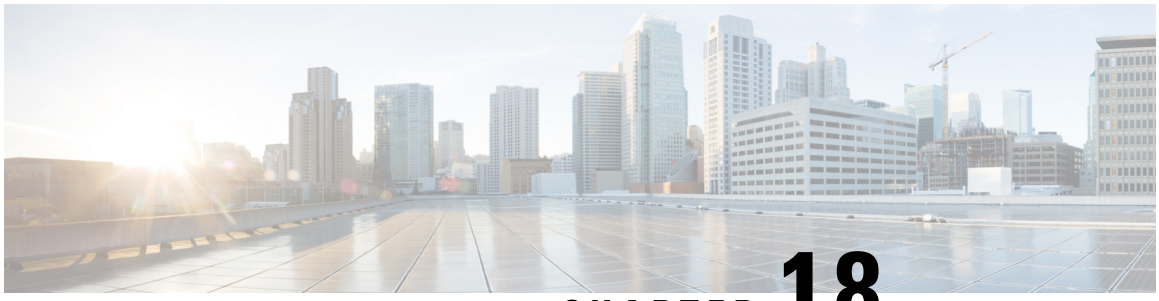
Feature Information for OSPFv3 ABR Type 3 LSA Filtering

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 19: Feature Information for OSPFv3 ABR Type 3 LSA Filtering

Feature Name	Releases	Feature Information
OSPFv3 ABR Type 3 LSA Filtering	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 18

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.
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:**	(Optional) Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Device(config-router-af)# end`	

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.
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.

	Command or Action	Purpose
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

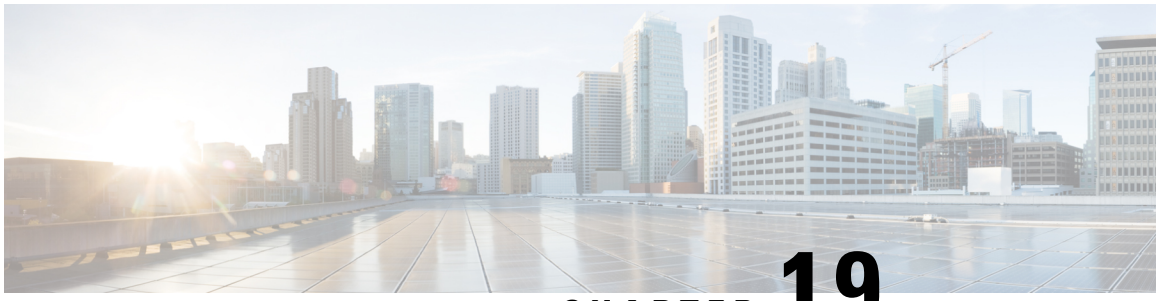
Feature Information for TTL Security Support for OSPFv3 on IPv6

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 20: TTL Security Support for OSPFv3 on IPv6

Feature Name	Software Releases	Feature Information
TTL Security Support for OSPFv3 on IPv6		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 19

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*
	Example:
	`Device(config)# ipv6 router ospf 1`
	Example:
	`Device(config)# router ospfv3 101`
		Enables OSPFv3 routing and enters router configuration mode.

Step 4	**shutdown** **Example:**	Shuts down the selected interface.

	Command or Action	Purpose
	`Device(config-router)# shutdown`	
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:**	Enables router configuration mode for the IPv6 address family.

	Command or Action	Purpose
	`Device(config)# router ospfv3 1`	
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.

	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 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`
	Example:
	`Device(config-if)# ospfv3 process-id ipv6 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.

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

Related Topic	Document Title
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

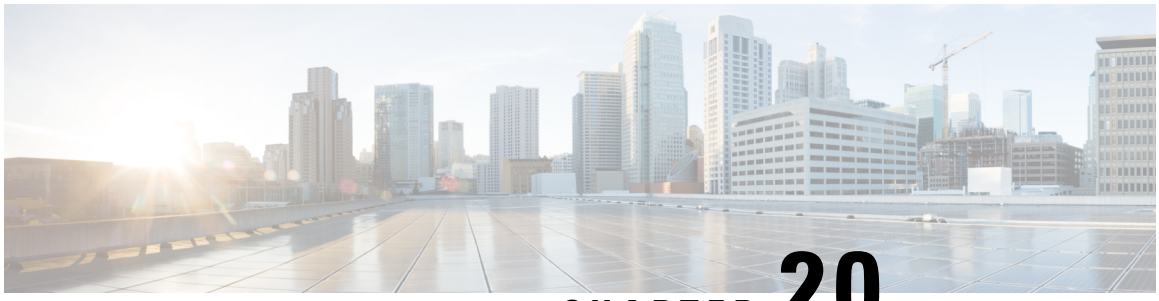
Feature Information for Graceful Shutdown Support for OSPFv3

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 21: Feature Information for Graceful Shutdown Support for OSPFv3

Feature Name	Releases	Feature Information
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. The following commands were introduced: • **ipv6 ospf shutdown** • **ospfv3 shutdown** • **shutdown (router ospfv3)**



CHAPTER 20

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** **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 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.
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:**	Displays general information about OSPFv3 routing processes.

	Command or Action	Purpose
	`Device# show ospfv3`	**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:**	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.

	Command or Action	Purpose
	`Device(config-if)# ospfv3 1 prefix-suppression disable`	
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:**	Displays information about the types of debugging that are enabled for your device.

	Command or Action	Purpose
	`Device# show debugging`	
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

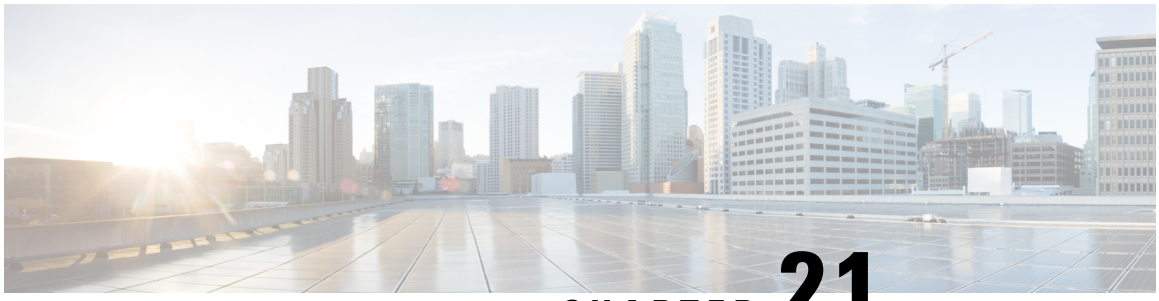
Feature Information for Prefix Suppression Support for OSPFv3

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 22: Feature Information for Prefix Suppression Support for OSPFv3

Feature Name	Releases	Feature Information
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). 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 21

Configuring OSPF Retransmissions Limit

OSPF Retransmissions Limit

The OSPF Retransmissions Limit feature adds a limit to the number of retransmissions of database exchange and update packets for both demand and non-demand circuits. The retransmission of these packets stops once this retry limit is reached, thus preventing unnecessary use of the link in continual retransmission of the packets if, for some reason, a neighbor is not responding during adjacency forming. This feature module describes the change in how the Open Shortest Path First (OSPF) protocol handles retransmissions.

Restrictions For OSPF Retransmissions Limit

The limit to the number of retransmissions does not apply for update packets on nonbroadcast multiaccess (NBMA) point-to-multipoint direct circuits. In this situation, the dead timer is used to end communication with non-responding neighbors and thus stop the retransmissions.

Information About OSPF Retransmissions Limit

Overview About OSPF Retransmissions Limit

There is a limit to the number of retransmissions of database exchange and update packets for both demand and non-demand circuits. The retransmission of these packets stops once this retry limit is reached, thus preventing unnecessary use of the link in continual retransmission of the packets if, for some reason, a neighbor is not responding during adjacency forming.

The limit for both demand circuit and non-demand circuit retransmissions is 24.

The limit-retransmissions command allows you to either remove (disable) the limit or change the maximum number of retransmissions to be a number from 1 to 255.

Benefits

The limit-retransmissions command provides for backward compatibility for previous or other releases of Cisco IOS or other routers that do not have this feature.

How to Configure OSPF Retransmissions Limit

Setting OSPF Retransmission Limits

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-ID*
4. **limit retransmissions**{[**dc** {*max-number* | **disable**}] [**non-dc** {*max-number* | **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	**router ospf** *process-ID* **Example:** `Device(config)#router ospf 18`	Configures OSPF routing process and enters OSPF router configuration mode.
Step 4	**limit retransmissions**{[**dc** {*max-number* | **disable**}] [**non-dc** {*max-number* | **disable**}]} **Example:** `Device(config-router)#limit retransmissions dc 5`	Sets the limit in the number of retransmissions of database exchange and update packets for both demand and non-demand circuits.
Step 5	**end** **Example:** `Device(config-router)#end`	Exits address router configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPF Retransmissions Limit

Example: Configuring OSPF Retransmissions Limit

The following is an example of configuring OSPF retransmissions limit.

```
router ospf 18
limit retransmissions dc 5
```

Additional References for OSPF Retransmissions Limit

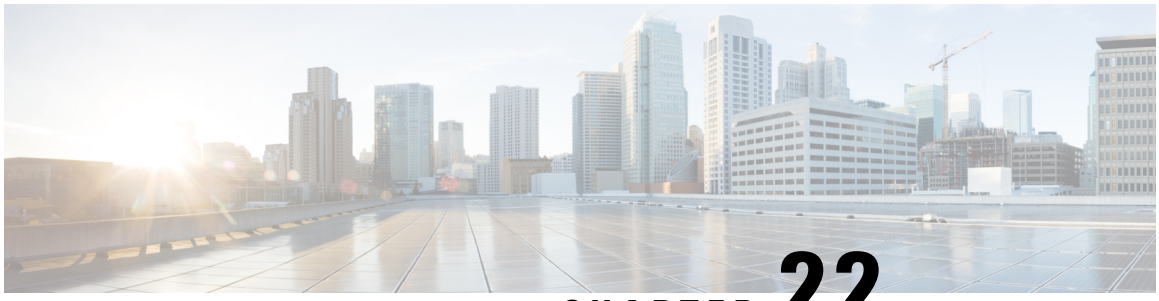
Related Documents

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

Feature Information for OSPF Retransmissions Limit

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.

Table 23: Feature Information for OSPF Retransmissions Limit



CHAPTER 22

OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

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

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

Prerequisites for Excluding Connected IP Prefixes from LSAs

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

Information About Excluding Connected IP Prefixes from LSAs

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

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

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

Feature Overview

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

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

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

Globally Suppressing IP Prefix Advertisements per OSPF Process

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

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

Suppressing IP Prefix Advertisements on a Per-Interface Basis

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

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

How to Exclude Connected IP Prefixes from OSPF LSAs

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

Excluding IP Prefixes per OSPF Process

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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	**prefix-suppression** **Example:** `Device(config-router)# prefix-suppression`	Prevents OSPF from advertising all IP 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 ip ospf** **Example:** `Device# show ip ospf`	Displays general information about OSPF routing processes. **Note** Use this command to verify that IP prefix suppression has been enabled.

Examples

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

```
Device# show ip ospf

Routing Process "ospf 1" with ID 10.0.0.6
Start time: 00:00:04.912, Time elapsed: 00:02:35.184
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
It is an area border router
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
```

```
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 2. Checksum Sum 0x0132C8
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 3. 3 normal 0 stub 0 nssa
Number of areas transit capable is 1
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Prefix-suppression is enabled
.
.
.
```

Excluding IP Prefixes on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `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:**	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf prefix-suppression** [**disable**] **Example:** `Device(config-if)# ip ospf prefix-suppression`	Prevents OSPF from advertising IP prefixes that belong to a specific interface, except those that are associated with secondary IP addresses.

	Command or Action	Purpose
		Note When you enter the **ip ospf prefix suppression**command in interface configuration mode, it takes precedence over the **prefix-suppression** command that is entered in router configuration mode.
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf interface** **Example:** `Device# show ip ospf interface`	Displays OSPF-related interface information. **Note** Use this command to verify that IP prefix suppression has been enabled for a specific interface.

Examples

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

```
Device# show ip ospf interface

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

Troubleshooting IP Prefix Suppression

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose
	`Device> enable`	
Step 2	**debug ip ospf lsa-generation** **Example:** `Device# debug ip ospf lsa-generation`	Displays informations about each OSPF LSA generated.
Step 3	**debug condition interface** *interface-type interface-number* [**dlci** *dlci*] [**vc** {*vci* | *vpi* | *vci*}] **Example:** `Device# debug interface serial 0/0`	Limits output for some **debug** commands on the basis of the interface or virtual circuit.
Step 4	**show debugging** **Example:** `Device# show debugging`	Displays information about the types of debugging that are enabled for your router.
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.

Examples

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

```
Device# debug ip ospf lsa-generation

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

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

Configuration Examples for Excluding Connected IP Prefixes from LSAs

Excluding IP Prefixes from LSAs for an OSPF Process Example

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

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

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

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

Excluding IP Prefixes from LSAs for a Specified Interface Example

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

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

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

```
Device# show ip ospf interface
```

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

Additional References

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

Related Documents

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

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
There are no new MIBs that are associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

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.

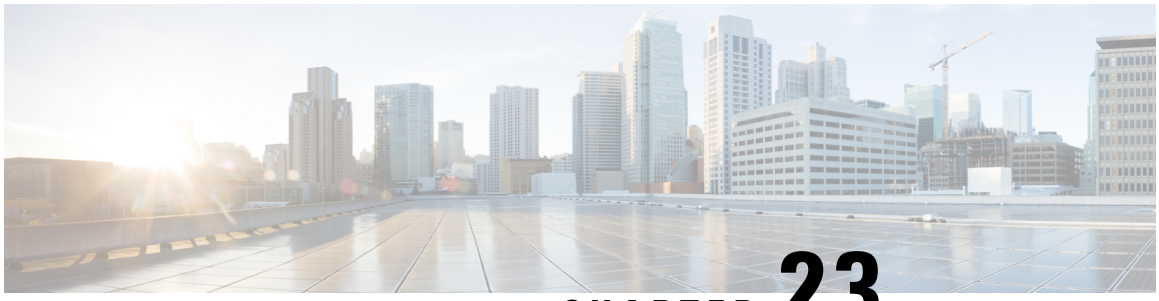
Table 24: Feature Information for OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements

Feature Name	Releases	Feature Information
OSPF Mechanism to Exclude Connected IP Prefixes from LSA Advertisements		The OSPF mechanism to exclude connected IP prefixes from LSA advertisements is deployed in large networks, limiting the number of IP prefixes that are carried in the OSPF LSAs can speed up OSPF convergence. No new commands were introduced or modified.

Glossary

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

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



CHAPTER 23

OSPF RFC 3623 Graceful Restart Helper Mode

OSPF RFC 3623 Graceful Restart Helper Mode

This document focuses on Nonstop Forwarding (NSF) helper mode for OSPFv2 in Cisco IOS software, using IETF standardized graceful restart helper mode functionality as described in RFC 3623, *Graceful OSPF Restart*. Graceful restart helper mode functionality, which is enabled by default, is useful for multiplatform network environments where helper mode routers on some platforms can assist restarting routers on mixed platforms that support OSPF graceful restart mode as well as helper mode.

Prerequisites for OSPF RFC 3623 Graceful Restart Helper Mode

- OSPF must be configured on the router.

Restrictions for OSPF RFC 3623 Graceful Restart Helper Mode

- IETF Graceful Restart is not supported over sham-links.

Information About OSPF RFC 3623 Graceful Restart Helper Mode

Cisco NSF Routing and Forwarding Operation

Prior to RFC 3623 Cisco implemented the Cisco proprietary NSF referred to as Cisco NSF. Users can configure either Cisco or RFC 3623 IETF NSF, depending on which versions are supported by the Cisco IOS software version running on the network. If the software version supports both types of NSF, you need to configure all routers with the same type of NSF.

Cisco NSF is supported by the BGP, EIGRP, OSPF, and IS-IS protocols for routing and by Cisco Express Forwarding (CEF) for forwarding. The BGP, EIGRP, OSPF, and IS-IS routing protocols have been enhanced with NSF capability and awareness, which means that routers that run these protocols can detect a switchover and take the necessary actions to continue forwarding network traffic and to recover route information from the neighbor routers.

In this document, a networking device is said to be NSF-aware if it is running NSF-compatible software. A device is said to be NSF-capable if it has been configured to support NSF; therefore, it would rebuild routing information from NSF-aware or NSF-capable neighbors. The NSF router mode of operation common to the Cisco and IETF NSF implementations is as follows:

- Restarting Mode--Also known as IETF NSF-restarting mode or graceful-restarting mode. In this mode, the OSPF router process is performing non-stop forwarding recovery because of an RP switchover; this may result from an RP crash or a software upgrade on the active RP.
- Helper Mode--Also known as IETF NSF-awareness. In this mode, the neighboring router is restarting and helping in the NSF recovery.

For more information about OSPF RFC 3623 Graceful Restart, see http://www.ietf.org/rfc/rfc3623.txt .

Cisco Express Forwarding for NSF

A key element of NSF is packet forwarding. The OSPF protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once OSPF has converged, CEF updates the Forwarding Information Base (FIB) table and removes stale route entries. CEF then updates the line cards with the new FIB information. CEF maintains the FIB and uses the FIB information that was current at the time of a switchover to continue forwarding packets during the switchover. This feature reduces traffic interruption during the switchover.

During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF keeps the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines can continue forwarding after a switchover as soon as the interfaces and a data path are available.

As the OSPF routing protocol starts to repopulate the RIB on a prefix-by-prefix basis, the updates in turn cause prefix-by-prefix updates that CEF uses to update the FIB and adjacency databases. Existing and new entries receive the new version number, indicating that they have been refreshed. The forwarding information is updated on the line cards or forwarding engines during convergence. The RP signals when the RIB has converged. The software removes all FIB and adjacency entries that have an epoch older than the current switchover epoch. The FIB now represents the newest routing protocol forwarding information.

The OSPF routing protocol runs on only the active RP, and OSPF receives routing updates from OSPF neighbor routers. The OSPF routing protocol does not run on the standby RP. Following a switchover, OSPF requests that the NSF-aware neighbor devices send state information to help rebuild the routing tables.

Note For NSF operation, OSPF depends on CEF to continue forwarding packets while OSPF rebuilds the routing information.

OSPF Graceful Restart Helper Mode Functionality per RFC 3623

Helper Mode Initiation

When a neighbor router that is on the same network segment as the restarting router receives a grace-LSA from the restarting router, the neighbor enters helper mode as long as the following criteria are met:

- The neighbor must have a full adjacency with the restarting router over the associated network segment.
- There have been no changes to the link-state database since the restarting router began restarting.
- The grace period has not yet expired.
- Local policy allows the neighbor router to act as a helper router.
- The neighbor router must not be in its own graceful restart process.
- Helper mode for this router has not been disabled by the network administrator.

Helper Mode Exit

The helper router stops performing helper mode for its neighbor when one of the following events occur:

- The grace-LSA that was originated by the restarting router is flushed, to signify that the restarting router has exited the graceful restart process successfully.
- The grace period of the grace-LSA expires.
- A change in link-state database contents indicates a network topology change, forcing the termination of the graceful restart process.

For complete information about graceful restart functionality, see RFC 3623 at http://www.ietf.org/rfc/rfc3623.txt .

The OSPF RFC 3623 Graceful Restart Helper Mode feature is enabled by default. Disabling this feature is not recommended because the disabled neighbor will detect the lost adjacency and the graceful restart process will be terminated on the restarting neighbor router.

The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. Strict LSA checking is disabled by default. You can enable strict LSA checking when there is a change to an LSA that would be flooded to the restarting router. You can configure strict LSA checking on both NSF-aware and NSF-capable routers; however, it becomes effective only when the router is in helper mode.

How to Use OSPF RFC 3623 Graceful Restart Helper Mode

Configuring Strict LSA Checking on the Helper Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **nsf ietf helper disable**
5. **nsf ietf helper strict-lsa-checking**
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	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 454`	Configures an Open Shortest Path First (OSPF) routing process and enters router configuration mode.
Step 4	**nsf ietf helper disable** **Example:** `Router(config-router)# nsf ietf helper disable`	Disables helper mode for IETF NSF.
Step 5	**nsf ietf helper strict-lsa-checking** **Example:** `Router(config-router)# nsf ietf strict-lsa-checking`	Enables strict LSA checking on an NSF-aware (helper) router.
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 454`	Displays general information about OSPF routing processes and whether helper mode or strict LSA checking is enabled for the NSF-aware (helper) router.

Configuration Examples for OSPF RFC 3623 Graceful Restart Helper Mode

Example Disabling Helper Support for IETF NSF

The following configuration example disables helper support for OSPF NSF.

```
Router(config)# router ospf 200
Router(config-router)# nsf ietf helper disable
```

Additional References

The following sections provide references related to the OSPF RFC 3623 Graceful Restart Helper Mode feature.

Related Documents

Related Topic	Document Title
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
OSPF configuration	"Configuring OSPF"
Cisco NSF feature in Cisco IOS software.	"Cisco Nonstop Forwarding"
Master list of Cisco IOS commands	Cisco IOS Master Command List, All Releases
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 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 RFC 3623 Graceful Restart Helper Mode

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 RFC 3623 Graceful Restart Helper Mode

Feature Name	Releases	Feature Information
OSPF RFC 3623 Graceful Restart Helper Mode	12.4(6)T	This document focuses on NSF for OSPFv2 in Cisco IOS software, using IETF standardized graceful restart functionality as described in RFC 3623. The following commands were introduced or modified: **nsf cisco helper disable**, **nsf ietf helper disable, nsf ietf helper strict-lsa-checking**.