IP Routing: OSPF Configuration Guide, Cisco IOS XE Release 2

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

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.

Finding Feature Information

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

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

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--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 BGP and EGP.
- 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. In Cisco IOS XE Release 3.3S and later releases, RFC 3101 replaces RFC 1587.
- OSPF over demand circuit--RFC 1793.

Configuration Limit on OSPF Links or Buffers

On systems with a large number of interfaces, OSPF can be configured such that the number of links advertised in the router link-state advertisement (LSA) causes the link state update packet to exceed the size of a "huge" Cisco IOS buffer. To solve 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.

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.

As with other routing protocols, enabling OSPF requires that you create an OSPF routing process, specify the range of IP addresses to be associated with the routing process, and assign area IDs to be associated with that range of IP addresses.

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, be sure that if you do configure any of these parameters, the configurations for all routers on your network have compatible values.

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 Frame Relay and SMDS) as broadcast networks. This feature saves you from needing to configure neighbors, as described in the section "Configuring OSPF for Nonbroadcast Networks, page 13" 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 or fully meshed network. This is not true for 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 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.

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

- Broadcast networks (GigabitEthernet, Token Ring, and FDDI)
- Nonbroadcast multiaccess (NBMA) networks (Switched Multimegabit Data Service [SMDS] and Frame Relay)
- 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.

Frame Relay provides an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. Refer to the **frame-relay map** command description in the *Cisco IOS Wide-Area Networking Command Reference* publication for more detail.

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 XE 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.

This feature allows the **neighbor** router configuration command to be used on point-to-multipoint interfaces.

On any point-to-multipoint interface (broadcast or not), the software assumed 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.

Our OSPF software allows you to configure several area parameters. These area parameters, shown in the following task table, include authentication, defining stub areas, and assigning specific costs to the default summary route. Authentication allows password-based protection against unauthorized access to an area.

Stub areas are areas into which information on external routes is not sent. Instead, there is a default external route generated by the ABR, into the stub area for destinations outside the autonomous system. To take advantage of the OSPF stub area support, *default routing* must be used in the stub area. To further reduce the number of LSAs sent into a stub area, you can configure the **no-summary** keyword of the **area stub**router configuration command on the ABR to prevent it from sending summary link advertisement (LSAs Type 3) into the stub area.

The OSPF NSSA feature is described by RFC 3101. In Cisco IOS Release XE3.3S and later releases, RFC 3101 replaces RFC 1587. RFC 3101 is backward compatible with RFC 1587. For a detailed list of differences between them, see Appendix F of RFC 3101. NSSA support was first integrated into Cisco IOS XE Release 2.1. OSPF NSSA is a nonproprietary extension of the existing OSPF stub area feature.

RFC 3101 support enhances both the Type 7 autonomous-system external routing calculation and the translation of Type 7 LSAs into Type 5 LSAs. For more information, see RFC 3101.

Use NSSA 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.

Cisco IOS Release XE3.3S and later releases support RFC 3101, which 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.

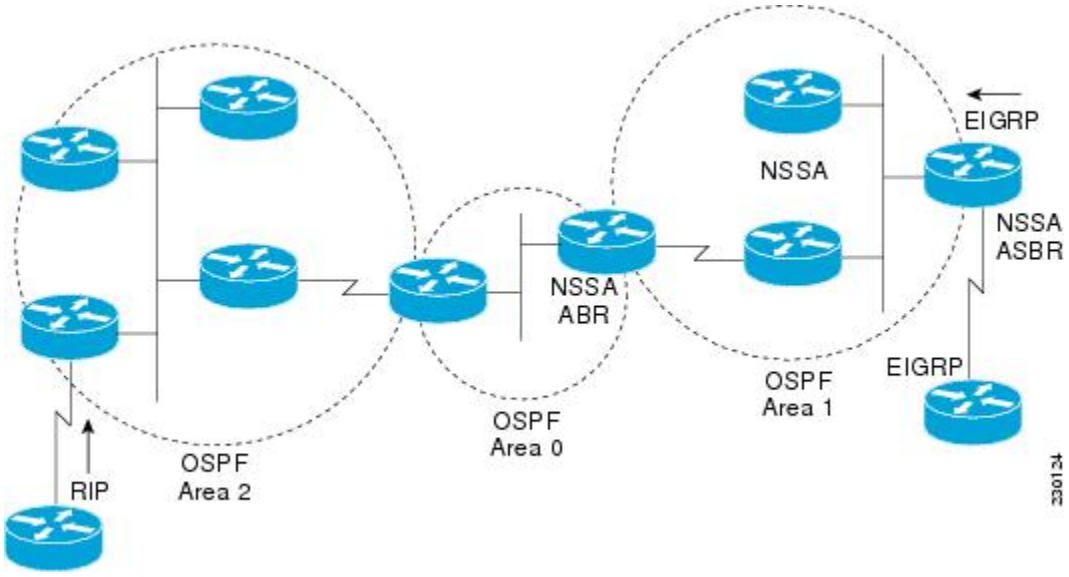
Note Even a forced translator might not translate all LSAs; translation depends on the contents of each LSA.

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.

Evaluate the following considerations before you implement OSPF NSSA:

- You can set a Type 7 default route that can be used to reach external destinations. If you do, the router generates a Type 7 default into the NSSA or the NSSA ABR.
- Every router within the same area must agree that the area is NSSA; otherwise, the routers will not be able to communicate.

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.

In Cisco IOS XE Release 3.3S and later releases, RFC 3101 replaces RFC 1587, and you can use the **always** keyword in the **area nssa translate** command to configure an NSSA ABR router as a forced NSSA LSA translator. This command will work if RFC 3101 is disabled and RFC 1587 is being used.

In Cisco IOS XE Release 3.3S and later releases, RFC 3101 replaces RFC 1587, and RFC 3101 behavior is automatically enabled. You can choose the route selection behavior by configuring a router to run as RFC 3101 or RFC 1587 compatible.

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 XE 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 *default route* 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 XE 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.

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 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 over 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, page 7
- LSA Group Pacing with Multiple Timers, page 8

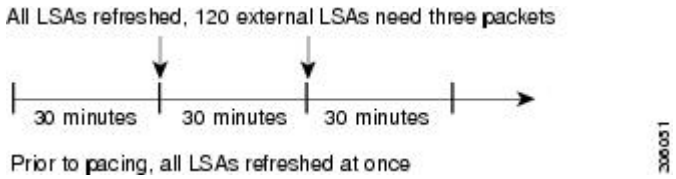
Original LSA Behavior

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 it generates and LSAs it receives from other routers. The router refreshes LSAs it generated; it ages the LSAs it received from other routers.

Prior to the LSA group pacing feature, the Cisco IOS XE 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 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 period of time.

Figure 2 OSPF LSAs on a Single Timer Without Group Pacing



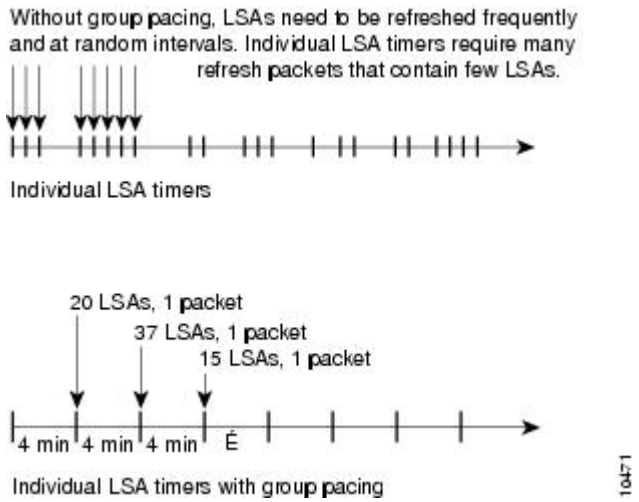
LSA Group Pacing with Multiple Timers

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 the router must send out, 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 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 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 of 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 the pacing is that OSPF update and retransmission packets are sent more efficiently.

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 first 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 Configuration Limit on OSPF Links or Buffers, page 2 section.

- Enabling OSPF, page 10
- Configuring OSPF Interface Parameters, page 11
- Configuring OSPF over Different Physical Networks, page 12
- Configuring OSPF Area Parameters, page 14

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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 109`	Enables OSPF routing, which places the router in router configuration mode.
Step 4	**network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(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:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring OSPF Interface Parameters

Command	Purpose
`Router(config-if)#` **ip ospf cost** *cost*	Explicitly specifies the cost of sending a packet on an OSPF interface.
`Router(config-if)#` **ip ospf retransmit-interval** *seconds*	Specifies the number of seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to an OSPF interface.
`Router(config-if)#` **i p ospf transmit-delay** *seconds*	Sets the estimated number of seconds required to send a link-state update packet on an OSPF interface.
`Router(config-if)#` **ip ospf priority** *number-value*	Sets priority to help determine the OSPF designated router for a network.
`Router(config-if)#` **ip ospf hello-interval** *seconds*	Specifies the length of time between the hello packets that the Cisco IOS XE software sends on an OSPF interface.
`Router(config-if)#` **ip ospf dead-interval** *seconds*	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.

Command	Purpose
`Router(config-if)#` **ip ospf authentication-key** *key*	Assigns a password to be used by neighboring OSPF routers on a network segment that is using the OSPF simple password authentication.
`Router(config-if)#` **ip ospf message-digest-key** *key-id* **md5** *key*	Enables OSPF MD5 authentication. The values for the *key-id* and *key* argumentsmust match values specified for other neighbors on a network segment.
`Router(config-if)#` **ip ospf authentication** [**message-digest** | **null**]	Specifies the authentication type for an interface.

Configuring OSPF over Different Physical Networks

Configuring Your OSPF Network Type

Command	Purpose
`Router(config-if)#` **ip ospf network** {**broadcast** | **non-broadcast** | {**point-to-multipoint** [**non-broadcast**] | **point-to-point**}}	Configures the OSPF network type for a specified interface.

Configuring Point-to-Multipoint Broadcast Networks

SUMMARY STEPS

1. **ip ospf network point-to-multipoint**
2. **exit**
3. **router ospf** *process-id*
4. **neighbor** *ip-address* **cost** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ip ospf network point-to-multipoint**	Configures an interface as point-to-multipoint for broadcast media.
Step 2	**exit**	Enters global configuration mode.
Step 3	**router ospf** *process-id*	Configures an OSPF routing process and enters router configuration mode.

	Command or Action	Purpose
Step 4	**neighbor** *ip-address* **cost** *number*	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

Command	Purpose
`Router(config-router)#` **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Configures a router interconnecting to nonbroadcast networks.

To treat the interface as point-to-multipoint when the media does not support broadcast, use the following commands beginning in interface configuration mode:

SUMMARY STEPS

1. Router(config-if)# **ip ospf network point-to-multipoint non-broadcast**
2. Router(config-if)# **exit**
3. Router(config)# **router ospf** *process-id*
4. Router(config-router)# **neighbor** *ip-address* [**cost** *number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config-if)# **ip ospf network point-to-multipoint non-broadcast**	Configures an interface as point-to-multipoint for nonbroadcast media.
Step 2	Router(config-if)# **exit**	Enters global configuration mode.
Step 3	Router(config)# **router ospf** *process-id*	Configures an OSPF routing process and enters router configuration mode.
Step 4	Router(config-router)# **neighbor** *ip-address* [**cost** *number*]	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

Command	Purpose
`Router(config-router)#` **area** *area-id* **authentication**	Enables authentication for an OSPF area.
`Router(config-router)#` **area** *area-id* **authentication message-digest**	Enables MD5 authentication for an OSPF area.
`Router(config-router)#` **area** *area-id* **stub** [**no-summary**]	Defines an area to be a stub area.
`Router(config-router)#` **area** *area-id* **default-cost** *cost*	Assigns a specific cost to the default summary route used for the stub area.

Configuring OSPF NSSA

Command	Purpose
`Router(config-router)#` **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]	Defines an area to be an NSSA.

To control summarization and filtering of Type 7 LSAs into Type 5 LSAs, use the following command in router configuration mode on the ASBR:

Command	Purpose
`Router(config-router)#` **summary address** *prefix mask* [**not advertise**] [**tag** *tag*]	Controls the summarization and filtering during the translation.

- Configuring an NSSA ABR as a Forced NSSA LSA Translator, page 14
- Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility, page 15

Configuring an NSSA ABR as a Forced NSSA LSA Translator

Note In Cisco IOS XE Release 3.3S and later releases, the output of the **show ip ospf** command shows whether the NSSA ABR is configured as a forced translator, and whether the router is running as RFC 3101 or RFC 1587 compatible.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**area** *area-id* **nssa translate type7 [always]** **Example:** `Router(config-router)# area 10 nssa translate type7 always`	Configures an NSSA ABR router as a forced NSSA LSA translator.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

Note In Cisco IOS XE Release 3.3S and later releases, the output of the **show ip ospf** command will indicate if the NSSA ABR is configured as RFC 3101 or RFC 1587 compatible.

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:** `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 and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**compatible rfc1587** **Example:** `Router(config-router)# compatible rfc1587`	Changes the method used to perform route selection to RFC 1587 compatibility and disables RFC 3101.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Configuring Route Summarization Between OSPF Areas

Configuring Route Summarization When Redistributing Routes into OSPF

Command	Purpose
`Router(config-router)#` **summary-address** {*ip-address mask* | *prefix mask*} [**not-advertise**] [**tag** *tag*]	Specifies an address and mask that covers redistributed routes, so only one summary route is advertised. Use the optional **not-advertise** keyword to filter out a set of routes.

Creating Virtual Links

Command	Purpose
`Router(config-router)#` **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*]	Creates a virtual link.

To display information about virtual links, use the **show ip ospf virtual-links** EXEC command. To display the router ID of an OSPF router, use the **show ip ospf** EXEC command.

Generating a Default Route

Command	Purpose
`Router(config-router)#` **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]	Forces the ASBR to generate a default route into the OSPF routing domain.

Configuring Lookup of DNS Names

Command	Purpose
ip ospf name-lookup	Configures DNS name lookup.

Forcing the Router ID Choice with a Loopback Interface

SUMMARY STEPS

1. **interface loopback 0**
2. **ip address** *ip-address mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface loopback 0**	Creates a loopback interface, which places the router in interface configuration mode.
Step 2	**ip address** *ip-address mask*	Assigns an IP address to this interface.

Controlling Default Metrics

Command	Purpose
`Router(config-router)#` **auto-cost reference-bandwidth** *ref-bw*	Differentiates high-bandwidth links.

Changing the OSPF Administrative Distances

Command	Purpose
`Router(config-router)#` **distance ospf** {**intra-area** | **inter-area** | **external**} *dist*	Changes the OSPF distance values.

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

Command	Purpose
timers spf *spf-delay spf-holdtime*	Configures route calculation timers.

Configuring OSPF over On-Demand Circuits

SUMMARY STEPS

1. Router(config)# **router ospf** *process-id*
2. Router(config)# **interface** *interface-type interface-number*
3. Router(config-if)# **ip ospf demand-circuit**

DETAILED STEPS

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

If the router is part of a point-to-point topology, then only one end of the demand circuit must be configured with this command. However, all routers must have this feature loaded.

If the router is part of a point-to-multipoint topology, only the multipoint end must be configured with this command.

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

- Prerequisites, page 19

Prerequisites

Evaluate the following considerations before implementing this 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.
- To take advantage of the on-demand circuit functionality within a stub area or NSSA, every router in the area must have this feature loaded. 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 the following document, *http://www.cisco.com/en/US/tech/*

tk365/technologies_tech_note09186a008009481b.shtml Why OSPF Demand Circuit Keeps Bringing Up the Link .

Logging Neighbors Going Up or Down

Command	Purpose
log-adjacency-changes [**detail**]	Sends syslog message when an OSPF neighbor goes up or down. **Note** Configure this command if you want to know about OSPF neighbors going up or down without turning on the **debug ip ospf adjacency** EXEC command. The **log-adjacency-changes** router configuration 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.

Changing the LSA Group Pacing Interval

Command	Purpose
`Router(config-router)#` **timers pacing lsa-group** *seconds*	Changes the group pacing of LSAs.

Blocking OSPF LSA Flooding

Command	Purpose
`Router(config-if)#` **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
`Router(config-router)#` **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.

Displaying OSPF Update Packet Pacing

Command	Purpose
`Router#` **show ip ospf flood-list** *interface-type interface-number*	Displays a list of LSAs waiting to be flooded over an interface.

Monitoring and Maintaining OSPF

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

Command	Purpose
`Router# show ip ospf [process-id [area-id]] database`	Displays lists of information related to the OSPF database.
`Router# show ip ospf [process-id [area-id]] database [database-summary]`	
`Router# show ip ospf [process-id [area-id]] database [router] [self-originate]`	
`Router# show ip ospf [process-id [area-id]] database [router] [adv-router [ip-address]]`	
`Router# show ip ospf [process-id [area-id]] database [router] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [network] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [summary] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [asbr-summary] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [external] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [nssa-external] [link-state-id]`	
`Router# show ip ospf [process-id [area-id]] database [opaque-link] [link-state-id]`	
`Router# show ip ospf [process-id`	

Command	Purpose
[*area-id*]] **database** [**opaque-area**] [*link-state-id*]	
Router# **show ip ospf** [*process-id* [*area-id*]] **database** [**opaque-as**] [*link-state-id*]	
Router# **show ip ospf flood-list interface** *interface-type*	Displays a list of LSAs waiting to be flooded over an interface (to observe OSPF packet pacing).
Router# **show ip ospf interface** [*interface-type interface-number*]	Displays OSPF-related interface information.
Router# **show ip ospf neighbor** [*interface-name*] [*neighbor-id*] **detail**	Displays OSPF neighbor information on a per-interface basis.
Router# **show ip ospf request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	Displays a list of all LSAs requested by a router.
Router# **show ip ospf retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]	Displays a list of all LSAs waiting to be re-sent.
Router# **show ip ospf** [*process-id*] **summary-address**	Displays a list of all summary address redistribution information configured under an OSPF process.
Router# **show ip ospf virtual-links**	Displays OSPF-related virtual links information.

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

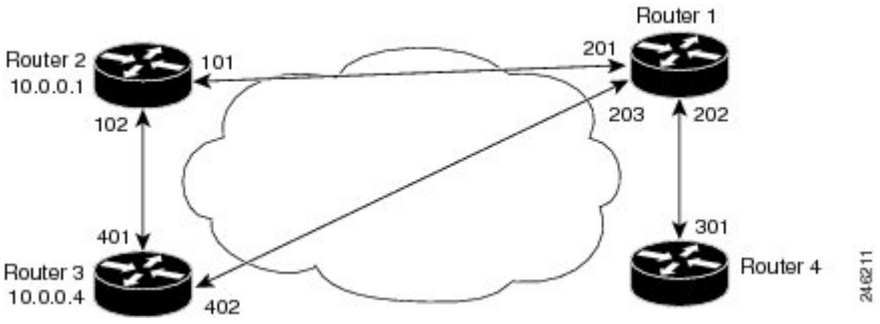
Command	Purpose
Router# **clear ip ospf** [*pid*] {**process** | **redistribution** | **counters** [**neighbor** [*neighbor-interface*] [*neighbor-id*]]*}*	Clears redistribution based on the OSPF routing process ID. If the *pid* option is not specified, all OSPF processes are cleared.

Configuration Examples for OSPF

Example OSPF Point-to-Multipoint

In the figure below, the router named Router 1 uses data-link connection identifier (DLCI) 201 to communicate with the router named Router 2, DLCI 202 to the router named Router 4, and DLCI 203 to the router named 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 1/0/0
 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 0/0/0
 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 3/0/0
 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 2/0/0
 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 Broadcast

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

```
interface Serial0/0/0
 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 0/0/0
 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:

```
Router# 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        Serial0/0/0
172.16.1.4        1   FULL/  -        00:01:47    10.0.1.4        Serial0/0/0
172.16.1.8        1   FULL/  -        00:01:45    10.0.1.3        Serial0/0/0
```

The route information in the first configuration is as follows:

```
Router# 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, Serial0/0/0
C       10.0.1.0/24 is directly connected, Serial0/0/0
O       10.0.1.5/32 [110/5] via 10.0.1.5, 00:39:08, Serial0/0/0
O       10.0.1.4/32 [110/10] via 10.0.1.4, 00:39:08, Serial0/0/0
```

Example OSPF Point-to-Multipoint Nonbroadcast

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

```
interface Serial0/0/0
 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 Serial9/2/1
 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:

```
Router# 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        Serial0/0/0
172.16.1.4        1   FULL/  -        00:01:52    10.0.1.4        Serial0/0/0
172.16.1.8        1   FULL/  -        00:01:52    10.0.1.3        Serial0/0/0
```

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 gigabitethernet 0/0/0
 ip address 172.16.10.1 255.255.255.0
! 8 bits of host address space reserved for ethernets
interface serial 0/0/0
 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 OSPF NSSA

In the following example, an OSPF stub network is configured to include OSPF Area 0 and OSPF Area 1, using five routers. OSPF Area 1 is defined as an NSSA, with Router 3 configured to be the NSSA ASBR and Router 2 configured to be the NSSA ABR. Following is the configuration output for the five routers.

Router 1

```
hostname Router1
!
interface Loopback1
 ip address 10.1.0.1 255.255.255.255
!
interface gigabitethernet 0/0/0
 ip address 192.168.0.1 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface Serial10/0/0
 description Router2 interface s11/0/0
 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
```

Router 2

```
hostname Router2
!
!
interface Loopback1
 ip address 10.1.0.2 255.255.255.255
!
interface Serial10/0/0
 description Router1 interface s11/0/0
 no ip address
```

```
 shutdown
 serial restart-delay 0
 no cdp enable
!
interface Serial11/0/0
 description Router1 interface s10/0/0
 ip address 192.168.10.2 255.255.255.0
 ip ospf 1 area 1
 serial restart-delay 0
 no cdp enable
!
interface Serial14/0/0
 description Router3 interface s13/0/0
 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
```

Router 3

```
hostname Router3
!
interface Loopback1
 ip address 10.1.0.3 255.255.255.255
!
interface gigabitethernet3/0/0
 ip address 192.168.3.3 255.255.255.0
 no cdp enable
!
interface Serial13/0/0
 description Router2 interface s14/0/0
 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
```

Router 4

```
hostname Router4
!
interface Loopback1
 ip address 10.1.0.4 255.255.255.255
!
interface gigabitethernet3/0/0
 ip address 192.168.3.4 255.255.255.0
 no cdp enable
!
interface gigabitethernet4/1/0
 ip address 192.168.41.4 255.255.255.0
!
router rip
 version 2
 network 192.168.3.0
 network 192.168.41.0
```

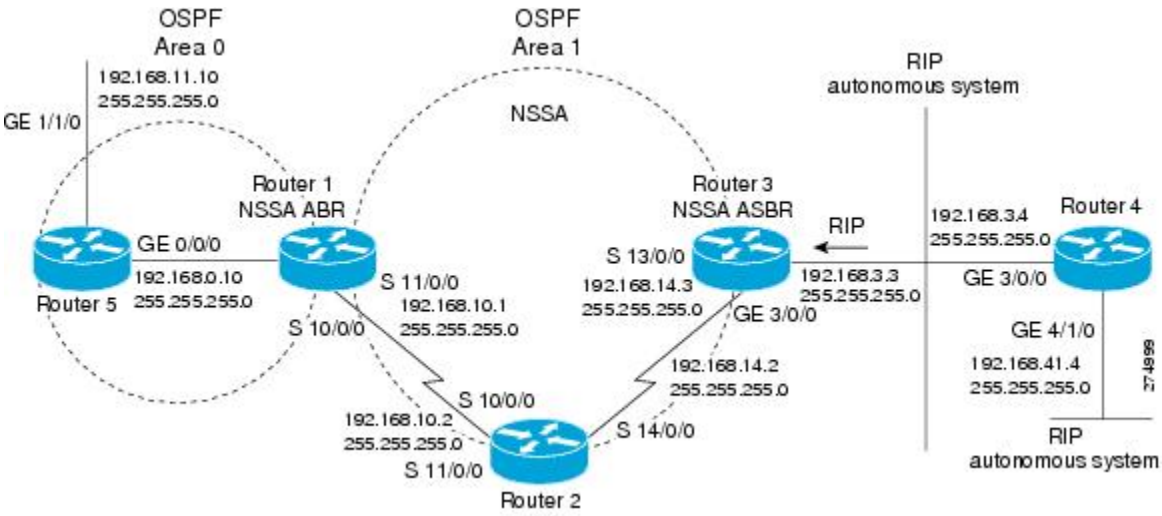
```
!
end
```

Router 5

```
hostname Router5
!
interface Loopback1
 ip address 10.1.0.5 255.255.255.255
!
interface gigabitethernet0/0/0
 ip address 192.168.0.10 255.255.255.0
 ip ospf 1 area 0
 no cdp enable
!
interface gigabitethernet1/1/0
 ip address 192.168.11.10 255.255.255.0
 ip ospf 1 area 0
!
router ospf 1
!
end
```

The figure below shows the OSPF stub network with NSSA Area 1. The redistributed routes that Router 4 is propagating from the two RIP networks will be translated into Type 7 LSAs by NSSA ASBR Router 3. Router 2, which is configured to be the NSSA ABR, will translate the Type 7 LSAs back to Type 5 so that they can be flooded through the rest of the OSPF stub network within OSPF Area 0.

Figure 5 OSPF NSSA Network with NSSA ABR and ASBR Routers



When the **show ip ospf** command is entered on Router 2, the output confirms that OSFP Area 1 is an NSSA area:

```
Router2# show ip ospf
 Routing Process "ospf 1" with ID 10.1.0.2
 Start time: 00:00:01.392, Time elapsed: 12:03:09.480
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 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
    Area 1
  Number of interfaces in this area is 2
! It is a NSSA area
  Area has no authentication
  SPF algorithm last executed 11:37:58.836 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 7. Checksum Sum 0x045598
  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
Router2# show ip ospf data
            OSPF Router with ID (10.1.0.2) (Process ID 1)
        Router Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Link count
10.1.0.1        10.1.0.1        1990        0x80000016 0x00CBCB 2
10.1.0.2        10.1.0.2        1753        0x80000016 0x009371 4
10.1.0.3        10.1.0.3        1903        0x80000016 0x004149 2
        Summary Net Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum
192.168.0.0     10.1.0.1        1990        0x80000017 0x00A605
192.168.11.0    10.1.0.1        1990        0x80000015 0x009503
        Type-7 AS External Link States (Area 1)
Link ID         ADV Router      Age         Seq#       Checksum Tag
192.168.3.0     10.1.0.3        1903        0x80000015 0x00484F 0
192.168.41.0    10.1.0.3        1903        0x80000015 0x00A4CC 0
```

Entering the **show ip ospf database data**command displays additional information about redistribution between Type 5 and Type 7 LSAs for routes that have been injected into the NSSA area and then flooded through the OSPF network.

```
Router2# show ip ospf database data
            OSPF Router with ID (10.1.0.2) (Process ID 1)
Area 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    2        0        0
     Prefixes redistributed in Type-7  0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Subtotal      7        0        0
Process 1 database summary
  LSA Type      Count    Delete   Maxage
  Router        3        0        0
  Network       0        0        0
  Summary Net   2        0        0
  Summary ASBR  0        0        0
  Type-7 Ext    2        0        0
  Opaque Link   0        0        0
  Opaque Area   0        0        0
  Type-5 Ext    0        0        0
      Prefixes redistributed in Type-5  0
  Opaque AS     0        0        0
  Total         7        0        0
```

Entering the **show ip ospf database nssa** command also displays detailed information for Type 7 to Type 5 translations:

```
Router2# show ip ospf database nssa
            OSPF Router with ID (10.1.0.2) (Process ID 1)
      Type-7 AS External Link States (Area 1)
  Routing Bit Set on this LSA
  LS age: 1903
  Options: (No TOS-capability, Type 7/5 translation, DC)
  LS Type: AS External Link
  Link State ID: 192.168.3.0 (External Network Number )
  Advertising Router: 10.1.0.3
  LS Seq Number: 80000015
  Checksum: 0x484F
  Length: 36
  Network Mask: /24
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 20
  Forward Address: 192.168.14.3
  External Route Tag: 0
  Routing Bit Set on this LSA
  LS age: 1903
! Options: (No TOS-capability, Type 7/5 translation, DC)
  LS Type: AS External Link
  Link State ID: 192.168.41.0 (External Network Number )
  Advertising Router: 10.1.0.3
  LS Seq Number: 80000015
  Checksum: 0xA4CC
  Length: 36
  Network Mask: /24
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 20
  Forward Address: 192.168.14.3
  External Route Tag: 0
```

Router 3

Entering the **show ip ospf** command on Router 3 displays the information to confirm that Router 3 is acting as an ASBR and that OSPF Area 1 has been configured to be an NSSA area:

```
Router3# show ip ospf
 Routing Process "ospf 1" with ID 10.1.0.3
 Start time: 00:00:01.392, Time elapsed: 12:02:34.572
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
!It is an autonomous system boundary router
 Redistributing External Routes from,
    rip, includes subnets in redistribution
 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
    Area 1
```

```
  Number of interfaces in this area is 1
! It is a NSSA area
  Area has no authentication
  SPF algorithm last executed 11:38:13.368 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 7. Checksum Sum 0x050CF7
  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
```

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 is for an OSPF NSSA area where RFC 3101 is disabled, RFC 1587 is active, and an NSSA ABR router is configured as a forced NSSA LSA translator. As described in the "Configuring OSPF NSSA", if RFC 3101 is disabled, the forced NSSA LSA translator remains inactive. The command output demonstrates this.

```
Router# 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 "Supports NSSA (compatible with RFC 1587)" line in the output indicates that RFC 1587 is active or that the OSPF NSSA area is RFC 1587 compatible.

The "Configured to translate Type-7 LSAs, inactive (RFC3101 support disabled)" line indicates that the OSPF NSSA area has an ABR router configured to act as a forced translator of Type 7 LSAs, but it is inactive because RFC 3101 is disabled.

```
Router2# 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 "Unconditional NSSA translator" line indicates that the status of the NSSA ASBR router is as a forced NSSA LSA translator.

Examples 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.

Basic OSPF Configuration Examples

The following example illustrates a simple OSPF configuration that enables OSPF routing process 9000, attaches GigabitEthernet interface 1/0/0 to area 0.0.0.0, and redistributes RIP into OSPF, and OSPF into RIP:

```
interface gigabitethernet 0/1/0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
!
interface gigabitethernet 1/0/0
 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
```

Basic OSPF Configuration for Internal Router for ABR and ASBRs Example

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 GigabitEthernet0/0/0 is in area 10.9.50.0:
interface gigabitethernet 0/0/0
 ip address 192.168.10.5 255.255.255.0
!
! Interface GigabitEthernet1/0/0 is in area 2:
interface gigabitethernet 1/0/0
 ip address 192.168.20.5 255.255.255.0
!
! Interface GigabitEthernet2/0/0 is in area 2:
interface gigabitethernet 2/0/0
 ip address 192.168.20.7 255.255.255.0
!
! Interface GigabitEthernet3/0/0 is in area 3:
interface gigabitethernet 3/0/0
 ip address 192.169.30.5 255.255.255.0
!
! Interface GigabitEthernet4/0/0 is in area 0:
interface gigabitethernet 4/0/0
 ip address 192.168.40.1 255.255.255.0
!
! Interface GigabitEthernet5/0/0 is in area 0:
interface gigabitethernet 5/0/0
 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 IOS XE software sequentially evaluates the address/wildcard-mask pair for each interface. See the **network area**command 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 GigabitEthernet interface 0/0/0. GigabitEthernet interface 0/0/0 is attached to area 10.9.50.0 only.

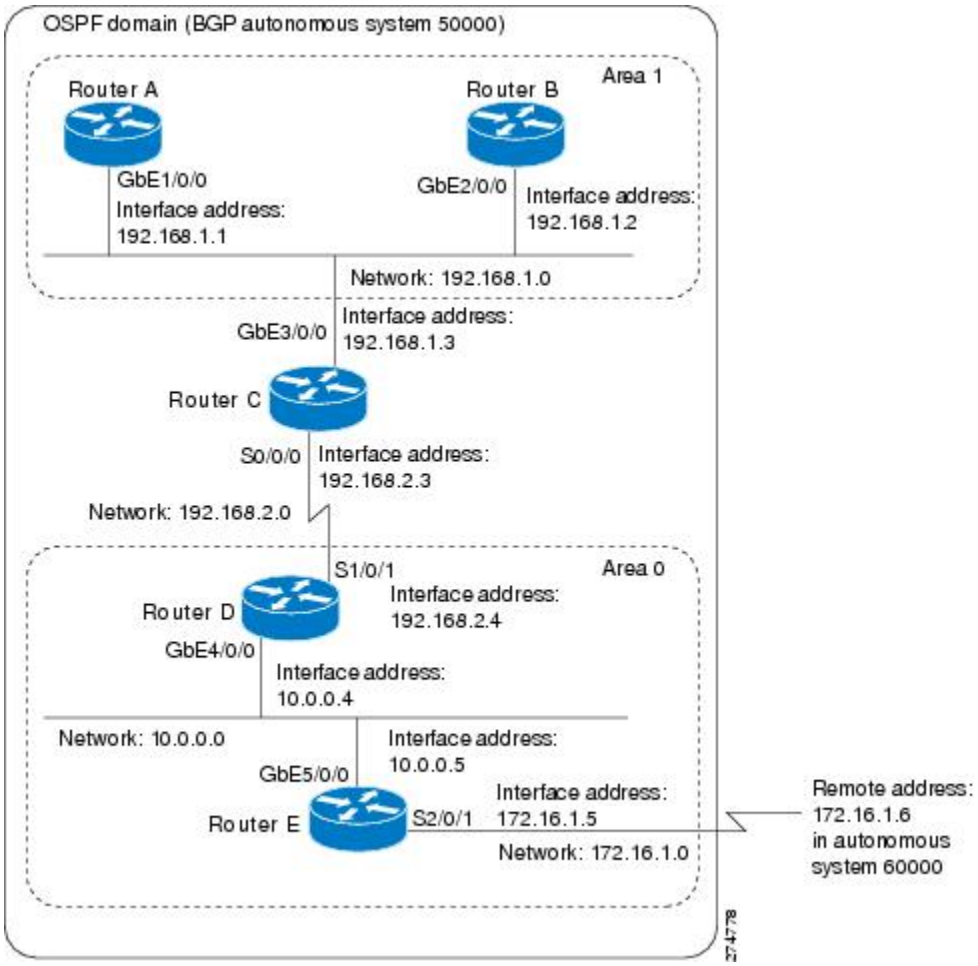
The second **network area**command is evaluated next. For area 2, the same process is then applied to all interfaces (except GigabitEthernet interface 0/0/0). Assume that a match is determined for interface GigabitEthernet 1/0/0. OSPF is then enabled for that interface and GigabitEthernet interface 1/0/0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

Complex Internal Router with ABR and ASBRs Example

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 example configuration.

Figure 6 Sample OSPF Autonomous System Network Map



In this configuration, five routers are configured with OSPF:

- Router A and Router Bare both internal routers within Area 1.
- Router C is an OSPF ABR. Note that for Router C, Area 1 is assigned to GbE3/0/0 and Area 0 is assigned to S0/0/0.
- 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. Example configurations follow.

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

Router A Configuration--Internal Router

```
interface gigabitethernet 1/0/0
 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 gigabitethernet 2/0/0
 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 gigabitethernet 3/0/0
 ip address 192.168.1.3 255.255.255.0
interface serial 0/0/0
 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 gigabitethernet 4/0/0
 ip address 10.0.0.4 255.0.0.0
interface serial 1/0/1
 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 gigabitethernet 5/0/0
 ip address 10.0.0.5 255.0.0.0
interface serial 2/0/1
 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
```

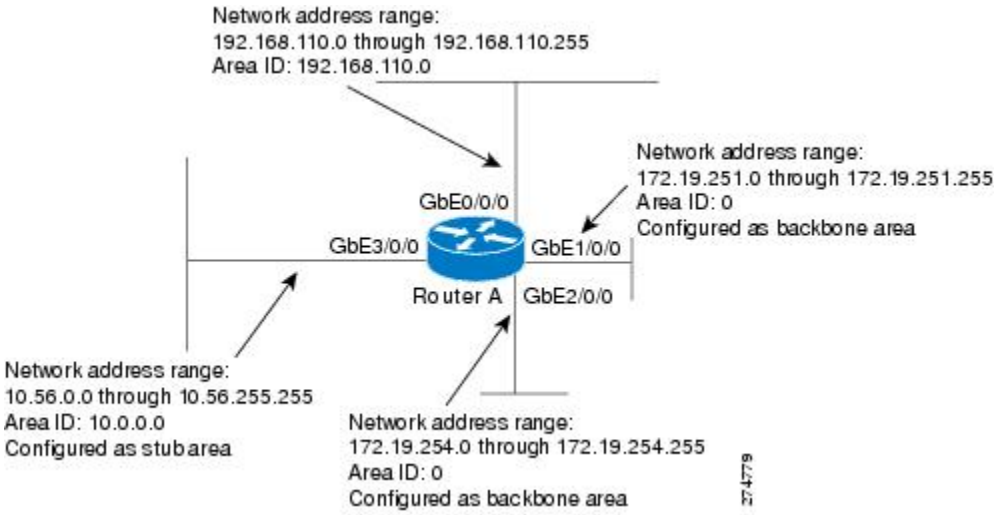
Complex OSPF Configuration for ABR Examples

The following example 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 7 Interface and Area Specifications for OSPF Example Configuration



The basic configuration tasks in this example are as follows:

- Configure address ranges for GigabitEthernet interface 0/0/0 through GigabitEthernet interface 3/0/0.
- 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 10.0.0.0. (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 **metric-type**, **metric**, **tag**, and **subnet**).
- Redistribute IGRP and OSPF into RIP.

The following is an example OSPF configuration:

```
interface GigabitEthernet 0/0/0
 ip address 192.42.110.201 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
```

```
interface gigabitethernet 1/0/0
 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 gigabitethernet 2/0/0
 ip address 172.19.254.2 255.255.255.0
 ip ospf authentication-key abcdefgh
 ip ospf cost 10
!
interface gigabitethernet 3/0/0
 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 both 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 192.89.0.0 and an ISO-IGRP learned route with prefix 49.0001.0002 will be 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 192.222.0.0 is in the routing table.

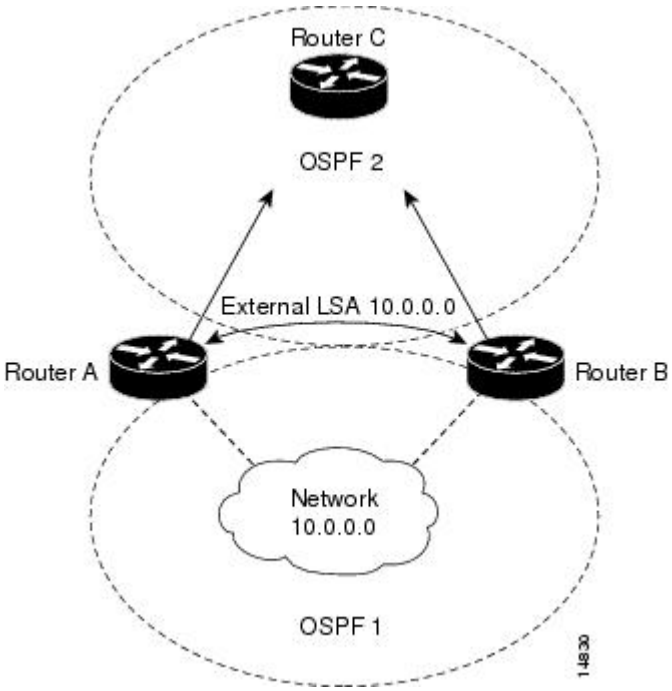
Note Only routes external to the OSPF process can be used for tracking, such as non-OSPF routes or OSPF routes from a separate OSPF process.

```
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 OSPF Administrative Distance

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

Figure 8 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 9 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 140.10.10.6 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 GigabitEthernet0/0/0
 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 Block LSA Flooding

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

```
interface gigabitethernet 0/0/0
 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: Ignore 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

The following sections provide references related to OSPF. To locate documentation of commands other than OSPF commands, use the command reference master index or search online.

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*
Protocol-independent features that work with OSPF	"Configuring IP Routing Protocol-Independent Features"

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, 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 1253	OSPF Version 2 Management Information Base, August 1991.
RFC 1587	The OSPF NSSA Option, March 1994
RFC 1793	Extending OSPF to Support Demand Circuits, April 1995
RFC 2328	OSPF Version 2, April 1998
RFC 3101	The OSPF NSSA Option, January 2003

Technical Assistance

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

Feature Information for OSPF

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

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

Table 1 Feature Information for OSPF

Feature Name	Releases	Feature Information
OSPF	Cisco IOS XE Release 2.1	OSPF is an IGP developed by the OSPF working group of the IETF. Designed expressly for IP networks, OSPF supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.
OSPF Flooding Reduction	Cisco IOS XE Release 2.1	The OSPF flooding reduction solution works by reducing unnecessary refreshing and flooding of already known and unchanged information. This feature is documented in the following section:

Feature Name	Releases	Feature Information
OSPF Not-So-Stubby Areas	Cisco IOS XE Release 2.1	OSPF NSSA is a nonproprietary extension of the existing OSPF stub area feature. This feature is documented in the following sections:
OSPF On Demand Circuit	Cisco IOS XE Release 2.1	OSPF on-demand circuit is an enhancement to the OSPF protocol that allows efficient operation over on-demand circuits such as ISDN and dialup lines. This feature is documented in the following sections:
OSPF Packet Pacing	Cisco IOS XE Release 2.1	OSPF update packets are automatically paced so they are not sent less than 33 milliseconds apart. This feature is documented in the following section:
OSPF-Demand Circuit Disable	Cisco IOS XE Release 3.2S	The **ignore** keyword was added to the **ip ospf demand-circuit** command, allowing you to prevent an interface from accepting demand-circuit requests from other routers.
OSPF Support for NSSA RFC 3101	Cisco IOS XE Release 3.3S	This feature adds support for the OSPF NSSA specification described by RFC 3101. RFC 3101 replaced RFC 1587 and is backward compatible with RFC 1587. The following commands were introduced or modified: **area nssa translate , compatible rfc1587**.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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, page 49
- Configuring Advertisement Until Routing Tables Converge, page 50
- Configuring Advertisement for a Graceful Shutdown, page 50
- Verifying the Advertisement of a Maximum Metric, page 51
- Monitoring and Maintaining OSPF Stub Router Advertisement, page 53

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.

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

The following sections provide references related to OSPF Stub Router Advertisement.

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

RFCs

RFC	Title
RFC 3137	OSPF Stub Router Advertisement

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 2 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**

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Restrictions on OSPF Update Packet-Pacing Configurable Timers

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

Information About OSPF Update Packet-Pacing Configurable Timers

Functionality of the OSPF Update Packet-Pacing Timers

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

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

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

Benefits of OSPF Update Packet-Pacing Configurable Timers

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

How to Configure OSPF Packet-Pacing Timers

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

Configuring OSPF Packet-Pacing Timers

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

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring a Retransmission Packet-Pacing Timer

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

SUMMARY STEPS

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

DETAILED STEPS

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

Configuring a Group Packet-Pacing Timer

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

SUMMARY STEPS

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

DETAILED STEPS

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

Verifying OSPF Packet-Pacing Timers

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

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

- Troubleshooting Tips, page 61

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 3 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**

OSPF Sham-Link Support for MPLS VPN

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

Finding Feature Information

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

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

Prerequisites for OSPF Sham-Link Support for MPLS VPN

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

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

Restrictions on OSPF Sham-Link Support for MPLS VPN

When OSPF is used as a protocol between PE and CE routers, the OSPF metric is preserved when routes are advertised over the VPN backbone. The metric is used on the remote PE routers to select the correct

route. For this reason, you should not modify the metric value when OSPF is redistributed to BGP, and when BGP is redistributed to OSPF. If you modify the metric value, routing loops may occur.

Information About OSPF Sham-Link Support for MPLS VPN

Benefits of OSPF Sham-Link Support for MPLS VPN

Client Site Connection Across the MPLS VPN Backbone

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

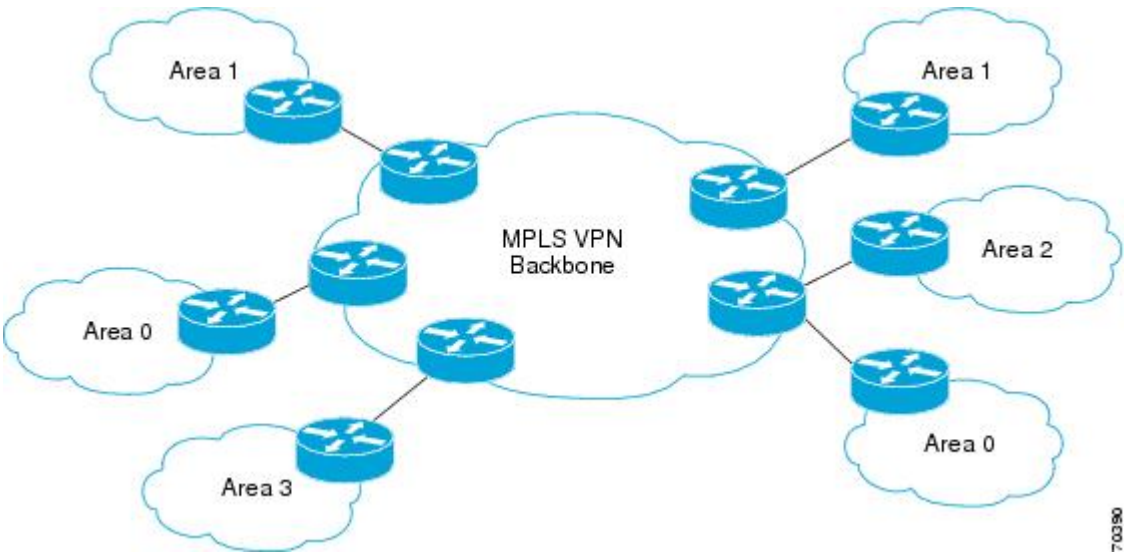
Flexible Routing in an MPLS VPN Configuration

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

Using OSPF in PE-CE Router Connections

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

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



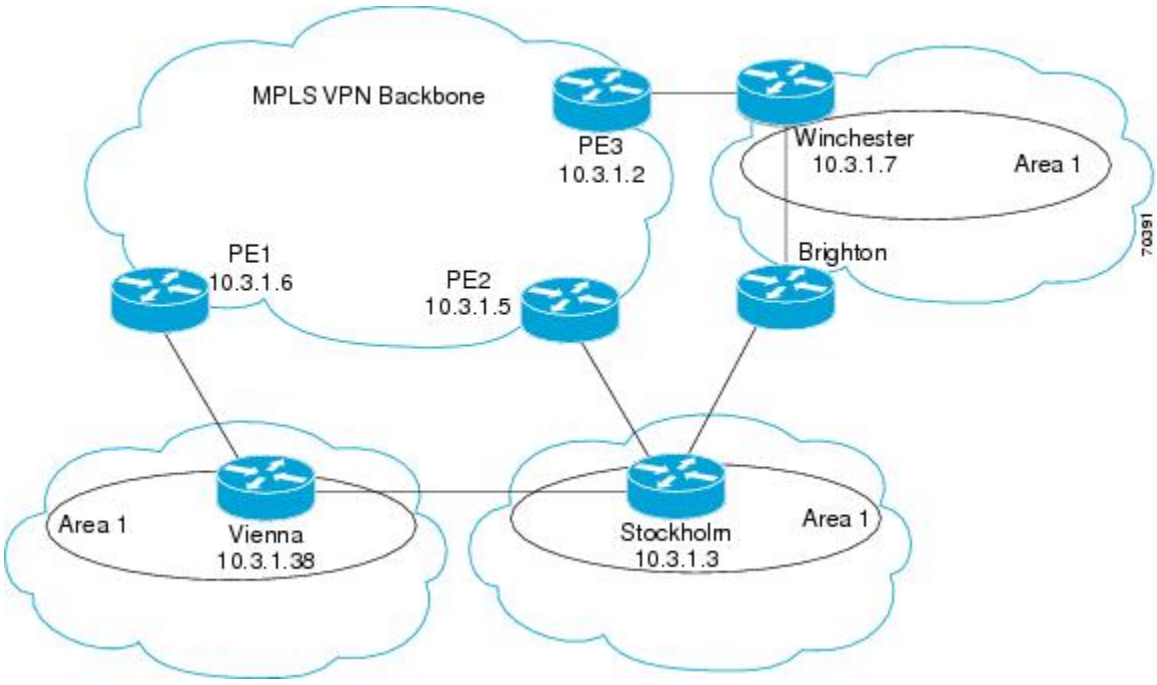
When OSPF is used to connect PE and CE routers, all routing information learned from a VPN site is placed in the VPN routing and forwarding (VRF) instance associated with the incoming interface. The PE routers that attach to the VPN use the Border Gateway Protocol (BGP) to distribute VPN routes to each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

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

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

Using a Sham-Link to Correct OSPF Backdoor Routing

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



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

The following example shows BGP routing table entries for the prefix 10.3.1.7/32 in the PE-1 router in the figure above. This prefix is the loopback interface of the Winchester CE router. As shown in bold in this

example, the loopback interface is learned via BGP from PE-2 and PE-3. It is also generated through redistribution into BGP on PE-1.

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

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

```
PE-1# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100", distance 110, metric 86, type intra area
  Redistributing via bgp 215
  Advertised by bgp 215
  Last update from 10.2.1.38 on Serial0/0/0, 00:00:17 ago
  Routing Descriptor Blocks:
  * 10.2.1.38
, from 10.3.1.7, 00:00:17 ago, via Serial0/0/0
      Route metric is 86, traffic share count is 1
```

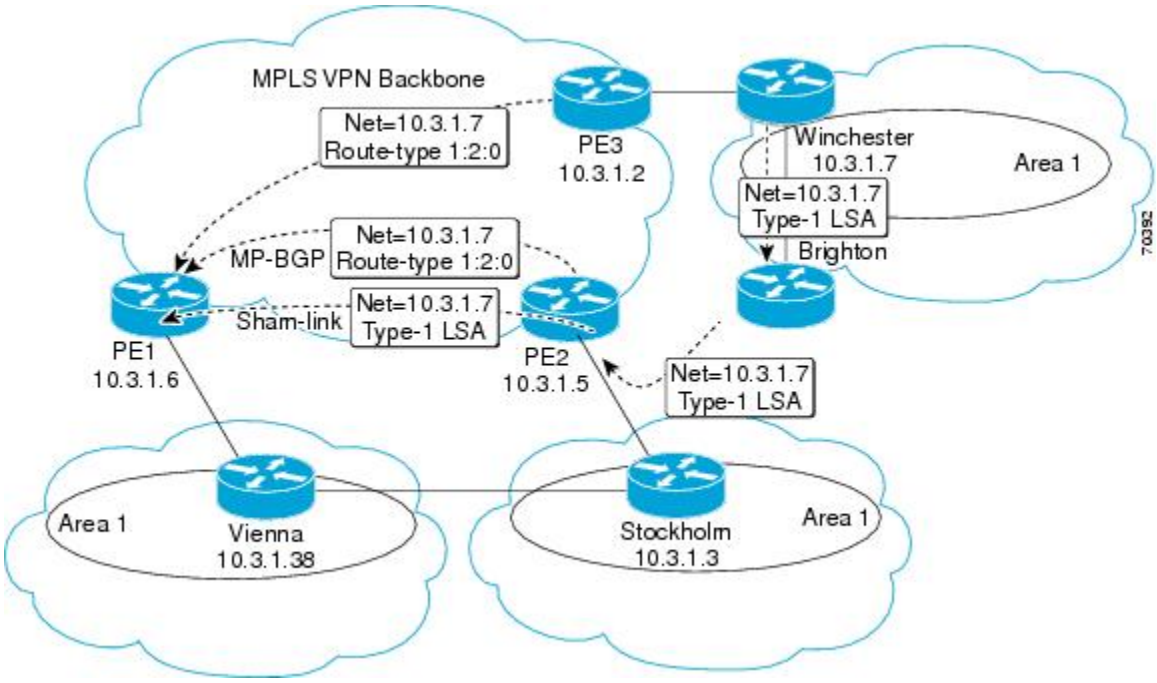
This path is selected because:

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

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

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

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



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

How to Configure an OSPF Sham-Link

Creating a Sham-Link

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

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

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router1# **configure terminal**	Enters global configuration mode on the first PE router.
Step 2	Router1(config)# **ip vrf** *vrf-name*	Defines a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.
Step 3	Router1(config-vrf)# **exit**	Exits VRF configuration mode and returns to global confiuration mode.
Step 4	Router1(config)# **interface loopback** *interface-number*	Creates a loopback interface to be used as an endpoint of the sham-link on PE-1 and enters interface configuration mode.
Step 5	Router1(config-if)# **ip vrf forwarding** *vrf-name*	Associates the loopback interface with a VRF. Removes the IP address.
Step 6	Router1(config-if)# **ip address** *ip-address mask*	Reconfigures the IP address of the loopback interface on PE-1.
Step 7	Router1(config-if)# **end**	Returns to global configuration mode.
Step 8	Router1(config)# **end**	Returns to EXEC mode.
Step 9	Router2# **configure terminal**	Enters global configuration mode on the second PE router.
Step 10	Router2(config)# **interface loopback** *interface-number*	Creates a loopback interface to be used as the endpoint of the sham-link on PE-2 and enters interface configuration mode.

	Command or Action	Purpose
Step 11	Router2(config-if)# **ip vrf forwarding** *vrf-name*	Associates the second loopback interface with a VRF. Removes the IP address.
Step 12	Router2(config-if)# **ip address** *ip-address mask*	Reconfigures the IP address of the loopback interface on PE-2.
Step 13	Router2(config-if)# **end**	Returns to global configuration mode.
Step 14	Router1(config)# **end**	Returns to EXEC mode.
Step 15	Router1(config)# **router ospf** *process-id* **vrf** *vrf-name*	Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-1 and enters interface configuration mode.
Step 16	Router1(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	Configures the sham-link on the PE-1 interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. **cost** *number* configures the OSPF cost for sending an IP packet on the PE-1 sham-link interface.
Step 17	Router2(config)# **router ospf** *process-id* **vrf** *vrf-name*	Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-2 and enters interface configuration mode.
Step 18	Router2(config-if)# **area** *area-id* **sham-link** *source-address destination-address* **cost** *number*	Configures the sham-link on the PE-2 interface within a specified OSPF area and with the loopback interfaces specified by the IP addresses as endpoints. **cost** *number* configures the OSPF cost for sending an IP packet on the PE-2 sham-link interface.

Verifying Sham-Link Creation

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

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

Monitoring and Maintaining a Sham-Link

Command	Purpose
Router# **show ip ospf sham-links**	Displays the operational status of all sham-links configured for a router.

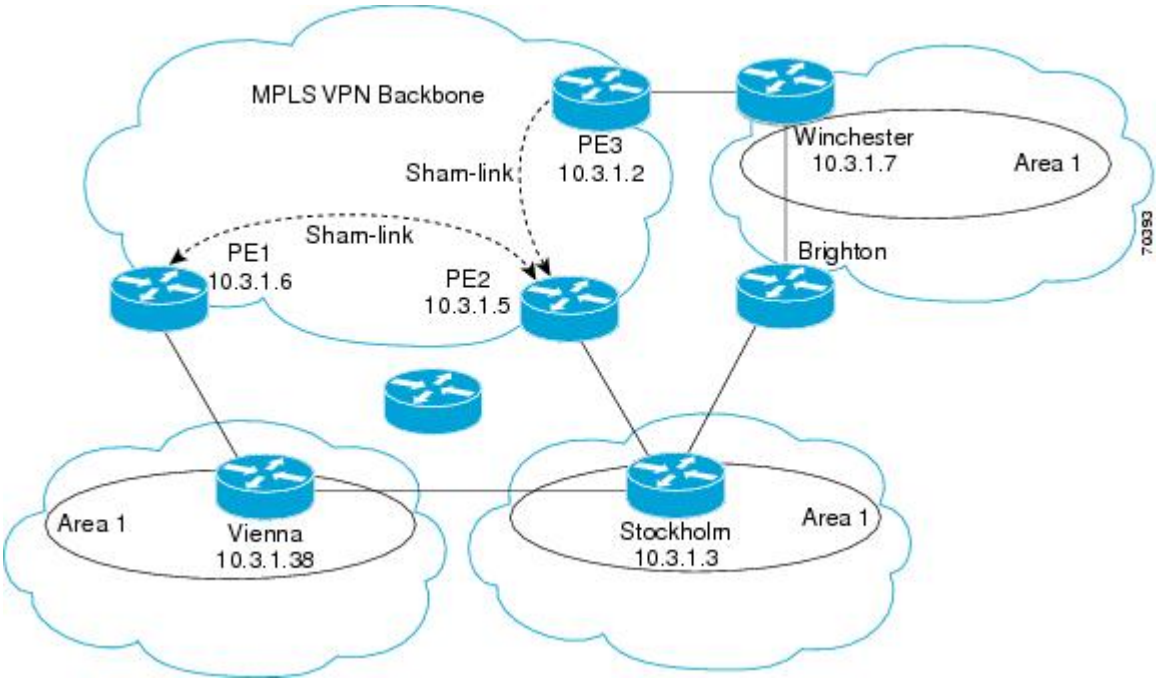
Command	Purpose
`Router#` **show ip ospf data router** *ip-address*	Displays information about how the sham-link is advertised as an unnumbered point-to-point connection between two PE routers.

Configuration Examples of an OSPF Sham-Link

Example Sham-Link Configuration

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

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



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

```
PE-1# show ip bgp vpnv4 all 10.3.1.7
```

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

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

```
PE-1# show ip bgp vpnv4 all tag | begin 10.3.1.7
   10.3.1.7/32      10.3.1.2
        notag/38

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

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

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

```
PE-2# show ip route vrf ospf 10.3.1.7
Routing entry for 10.3.1.7/32
  Known via "ospf 100
", distance 110, metric 12, type intra area
  Redistributing via bgp 215
  Last update from 10.3.1.2 00:00:10 ago
  Routing Descriptor Blocks:
  * 10.3.1.2 (Default-IP-Routing-Table), from 10.3.1.7, 00:00:10 ago
      Route metric is 12, traffic share count is 1
PE-2# show ip bgp vpnv4 all 10.3.1.7
BGP routing table entry for 100:251:10.3.1.7/32, version 166
Paths: (1 available, best #1)
```

```
  Not advertised to any peer
  Local
    10.3.1.2 (metric 30) from 10.3.1.2 (10.3.1.2)
      Origin incomplete, metric 11, localpref 100, valid, internal,
      best
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

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

Example Sham-Link Between Two PE Routers

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

```
Router1(config)
# interface loopback 1
Router1(config-if)# ip vrf forwarding ospf
Router1(config-if)# ip address 10.2.1.1 255.255.255.255
!
Router2(config)# interface loopback 1
Router2(config-if)# ip vrf forwarding ospf
Router2(config-if)# ip address 10.2.1.2 255.255.255.255
!
Router1(config)# router ospf 100 vrf ospf
Router1(config-if)# area 1 sham-link 10.2.1.1 10.2.1.2 cost 40
!
Router2(config)# router ospf 100 vrf ospf
Router2(config-if)# area 1 sham-link 10.2.1.2 10.2.1.1 cost 40
```

Additional References

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

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases
MPLS Virtual Private Networks	"MPLS Virtual Private Networks"

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 1163	*A Border Gateway Protocol*
RFC 1164	*Application of the Border Gateway Protocol in the Internet*
RFC 2283	*Multiprotocol Extensions for BGP-4*
RFC 2328	*Open Shortest Path First, Version 2*
RFC 2547	*BGP/MPLS VPNs*

Technical Assistance

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

Feature Information for OSPF Sham-Link Support for MPLS VPN

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

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

Table 4 Feature Information for OSPF Sham-Link Support for MPLS VPN

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

Glossary

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

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

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

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

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

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

OSPF --Open Shortest Path First protocol.

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

SPF --shortest path first calculation.

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

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

OSPF Support for Multi-VRF on CE Routers

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

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

Finding Feature Information

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

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

Information About OSPF Support for Multi-VRF on CE Routers

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

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

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

Configuring the Multi-VRF Capability for OSPF Routing

CEF must be running on the network.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf** [*process-id* **Example:** `Router# show ip ospf 1`	Displays the status of the router. If the display indicates that the router is connected to the VPN backbone, you can use the **capability vrf-lite** command to decouple the PE router from the VPN backbone.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

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

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

Verifying the OSPF Multi-VRF Configuration

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

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

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

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

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

Example Configuring the Multi-VRF Capability

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

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

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

Additional References

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

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"
Multiprotocol Label Switching (MPLS)	*Cisco IOS XE Multiprotocol Label Switching Configuration Guide, Release 2*
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

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

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

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

Table 5 Feature Information for OSPF Support for Multi-VRF on CE Routers

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

Glossary

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

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

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

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

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

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

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

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

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

VRF --VPN Routing and Forwarding.

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.

Finding Feature Information

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

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

Prerequisites for OSPF Forwarding Address Suppression

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

Information About OSPF Forwarding Address Suppression

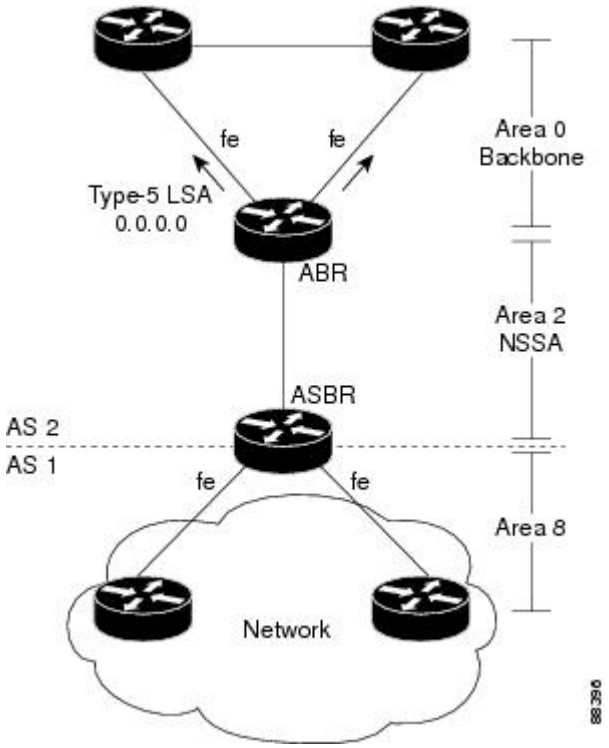
Benefits of OSPF Forwarding Address Suppression

The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes an NSSA ABR to translate Type-7 LSAs to Type-5 LSAs, but use the 0.0.0.0 as the forwarding address instead of that specified in the Type-7 LSA. This feature causes 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 10 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 the OSPF Forwarding Address

- Suppressing the OSPF Forwarding Address in Translated Type-5 LSAs, page 89

Suppressing the OSPF Forwarding Address in Translated Type-5 LSAs

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

Caution Configuring this feature causes the 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:** `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.

	Command or Action	Purpose
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**area** *area-id* **nssa translate type7 suppress-fa** **Example:** `Router(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:** `Router(config-router)# end`	Exits configuration mode and returns to privileged EXEC mode.

Configuration Examples for OSPF Forwarding Address Suppression

Suppressing OSPF Forwarding Address in Translated Type-5 LSAs Example

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for OSPF Forwarding Address Suppression

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

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

Table 6 Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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

OSPF Inbound Filtering Using Route Maps with a Distribute List

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

Finding Feature Information

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

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

Prerequisites OSPF Inbound Filtering Using Route Maps with a Distribute List

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

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

Benefits of OSPF Route-Map-Based-Filtering

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

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

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

Filtering Based on Route Tag

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

Filtering Based on Route Type

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

Filtering Based on Route Source

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

Filtering Based on Interface

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

Filtering Based on Next-Hop

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

How to Configure OSPF Inbound Filtering Using Route Maps

- Configuring OSPF Inbound Filtering Using a Route Map, page 97

Configuring OSPF Inbound Filtering Using a Route Map

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [**permit**	**deny**] [*sequence-number*] **Example:** `Router(config)# route-map tag-filter deny 10`	Defines a route map to control filtering.

	Command or Action	Purpose

Step 4	**match tag** *tag-name*
	
	Example:
	
	Example:
	`or other` **match** `commands`
	
	Example:
	`Router(config-router)# match tag 777`
		Matches routes with a specified name, to be used as the route map is referenced.
		• At least one **match** command is required, but it need not be this **match**command. This is just an example.
		• The list of **match** commands available to be used in this type of route map appears on the **distribute-list in** command reference page.
		• This type of route map will have no **set** commands.

Step 5	Repeat Steps 3 and 4 with other **route-map** and **match** commands if you choose.	--
Step 6	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode.
Step 7	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 8	**distribute-list route-map** *map-tag* **in** **Example:** `Router(config-router)# distribute-list route-map tag-filter in`	Enables filtering based on an OSPF route map.
Step 9	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

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

Example OSPF Route-Map-Based Filtering

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

```
route-map tag-filter deny 10
 match tag 777
route-map tag-filter permit 20
!
router ospf 1
 router-id 10.0.0.2
 log-adjacency-changes
 network 172.16.2.1 0.0.0.255 area 0
 distribute-list route-map tag-filter in
```

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

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

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

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

Table 7 Feature Information for OSPF Inbound Filtering Using Route Maps with a Distribute List

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

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Information About OSPF SPF Throttling

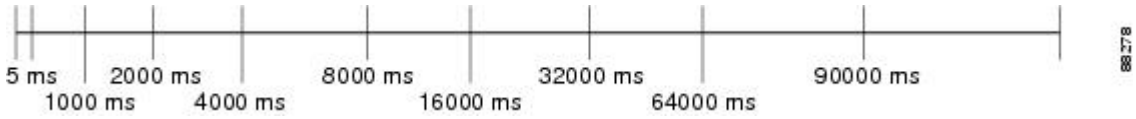
SPF calculations occur at the interval set by the **timers throttle spf**command. The wait interval indicates the amount of time to wait until the next SPF calculation occurs. Each wait interval after that calculation is twice as long as the previous one until the wait interval reaches the maximum wait 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 11 SPF Calculation Intervals Set by the timers throttle spf Command

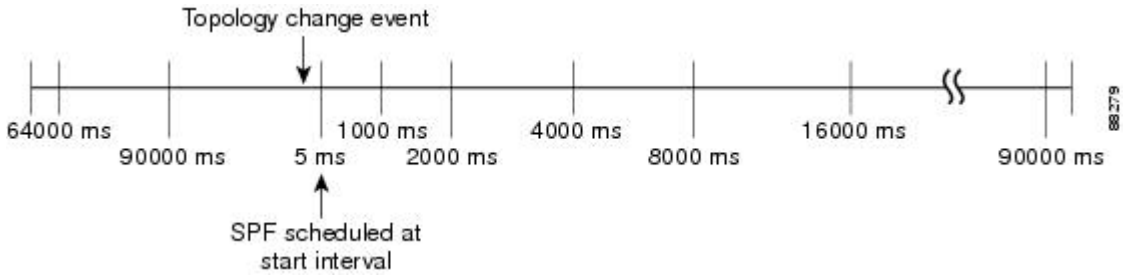


Notice that the wait interval between SPF calculations doubles when at least one topology change event is received during the previous wait interval. Once the maximum wait time is reached, the wait interval remains the same until the topology stabilizes and no event is received in that interval.

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 12 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 8 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**

OSPF Support for Fast Hello Packets

The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration results in faster convergence in an Open Shortest Path First (OSPF) network.

Finding Feature Information

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

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

Prerequisites for OSPF Support for Fast Hello Packets

OSPF must be already configured in the network or must be configured at the same time as the OSPF Support for Fast Hello Packets feature.

Information About OSPF Support for Fast Hello Packets

OSPF Hello Interval and Dead Interval

OSPF hello packets are packets that an OSPF process sends to its OSPF neighbors to maintain connectivity with those neighbors. The hello packets are sent at a configurable interval (in seconds). The defaults are 10 seconds for an Ethernet link and 30 seconds for a non broadcast link. Hello packets include a list of all neighbors for which a hello packet has been received within the dead interval. The dead interval is also a configurable interval (in seconds), and defaults to four times the value of the hello interval. The value of all hello intervals must be the same within a network. Likewise, the value of all dead intervals must be the same within a network.

These two intervals work together to maintain connectivity by indicating that the link is operational. If a router does not receive a hello packet from a neighbor within the dead interval, it will declare that neighbor to be down.

OSPF Fast Hello Packets

OSPF fast hello packets refer to hello packets being sent at intervals of less than 1 second. To understand fast hello packets, you should already understand the relationship between OSPF hello packets and the dead interval. See the section OSPF Hello Interval and Dead Interval, page 110.

OSPF fast hello packets are achieved by using the **ip ospf dead-interval** command. The dead interval is set to 1 second, and the hello-multiplier value is set to the number of hello packets you want to send during that 1 second, thus providing subsecond or "fast" hello packets.

When fast hello packets are configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

The dead interval must be consistent on a segment, whether it is set to 1 second (for fast hello packets) or set to any other value. The hello multiplier need not be the same for the entire segment as long as at least one hello packet is sent within the dead interval.

Benefits of OSPF Fast Hello Packets

The benefit of the OSPF Support for Fast Hello Packets feature is that your OSPF network will experience faster convergence time than it would without fast hello packets. This feature allows you to detect lost neighbors within 1 second. It is especially useful in LAN segments, where neighbor loss might not be detected by the Open System Interconnection (OSI) physical layer and data-link layer.

How to Configure OSPF Fast Hello Packets

- Configuring OSPF Fast Hello Packets, page 111

Configuring OSPF Fast Hello Packets

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf dead-interval minimal hello-multiplier** *multiplier*
5. **end**
6. **show ip ospf interface** [*interface-type interface-number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface gigabitethernet 0/0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip ospf dead-interval minimal hello-multiplier** *multiplier* **Example:** `Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5`	Sets the interval during which at least one hello packet must be received, or else the neighbor is considered down. • In the example, OSPF Support for Fast Hello Packets is enabled by specifying the **minimal** keyword and the **hello-multiplier** keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode. • Use this command when you are ready to exit configuration mode and save the configuration to the running configuration file.

Command or Action	Purpose
Step 6 **show ip ospf interface** [*interface-type interface-number*] **Example:** `Router# show ip ospf interface gigabitethernet 0/0/1`	(Optional) Displays OSPF-related interface information. • The relevant fields that verify OSPF fast hello packets are indicated in the sample output following this table.

Examples

The following sample output verifies that OSPF Support for Fast Hello Packets is configured. In the line that begins with "Timer intervals configured," the hello interval is 200 milliseconds, the dead interval is 1 second, and the next hello packet is due in 76 milliseconds.

```
Router# show ip ospf interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet Address 172.16.1.2/24, Area 0
  Process ID 1, Router ID 172.17.0.2, Network Type BROADCAST, Cost:1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 172.17.0.2, Interface address 172.16.1.2
  Backup Designated router (ID) 172.16.0.1, Interface address 172.16.1.1
  Timer intervals configured, Hello 200 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 76 msec
Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.0.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

Configuration Examples for OSPF Support for Fast Hello Packets

Example OSPF Fast Hello Packets

The following example configures OSPF fast hello packets; the dead interval is 1 second and 5 hello packets are sent every second:

```
interface gigabitethernet 0/0/1
 ip ospf dead-interval minimal hello-multiplier 5
```

Additional References

The following sections provide references related to OSPF Support for Fast Hello Packets.

Related Documents

Related Topic	Document Title
OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring OSPF	"Configuring OSPF"
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

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

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPF Support for Fast Hello Packets

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

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

Table 9 Feature Information for OSPF Support for Fast Hello Packets

Feature Name	Releases	Feature Information
OSPF Support for Fast Hello Packets	Cisco IOS XE Release 2.1	The OSPF Support for Fast Hello Packets feature provides a way to configure the sending of hello packets in intervals less than 1 second. Such a configuration results in faster convergence in an Open Shortest Path First (OSPF) network.

OSPF Incremental SPF

The Open Shortest Path First (OSPF) protocol can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event.

Finding Feature Information

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

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

Prerequisites for OSPF Incremental SPF

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

Information About OSPF Incremental SPF

OSPF uses Dijkstra's SPF algorithm to compute the shortest path tree (SPT). During the computation of the SPT, the shortest path to each node is discovered. The topology tree is used to populate the routing table with routes to IP networks. When changes to a Type-1 or Type-2 link-state advertisement (LSA) occur in an area, the entire SPT is recomputed. In many cases, the entire SPT need not be recomputed because most of the tree remains unchanged. Incremental SPF allows the system to recompute only the affected part of the tree. Recomputing only a portion of the tree rather than the entire tree results in faster OSPF convergence and saves CPU resources. Note that if the change to a Type-1 or Type-2 LSA occurs in the calculating router itself, then the full SPT is performed.

Incremental SPF is scheduled in the same way as the full SPF. Routers enabled with incremental SPF and routers not enabled with incremental SPF can function in the same internetwork.

How to Enable OSPF Incremental SPF

Enabling Incremental SPF

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**ispf** **Example:** `Router(config-router)# ispf`	Enables incremental SPF.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Incremental SPF

Example Incremental SPF

This example enables incremental SPF:

```
router ospf 1
 ispf
```

Additional References

The following sections provide references related to OSPF Incremental SPF.

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for OSPF Incremental SPF

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

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

Table 10 Feature Information for OSPF Incremental SPF

Feature Name	Releases	Feature Information
OSPF Incremental SPF	Cisco IOS XE Release 2.1	OSPF can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is more efficient than the full SPF algorithm, thereby allowing OSPF to converge faster on a new routing topology in reaction to a network event The following commands are introduced or modified in the feature documented in this module: • **ispf**

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for OSPF 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 someone mistakenly injects a large number of IP routes into OSPF, perhaps by redistributing Border Gateway Protocol (BGP) into OSPF, the network can be severely flooded. Limiting the number of redistributed routes prevents this potential problem.

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.

	Command or Action	Purpose
Step 4	**redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router)# redistribute eigrp 10`	Redistributes routes from one routing domain into another routing domain.
Step 5	**redistribute maximum-prefix** *maximum* [*threshold*] **Example:** `Router(config-router)# redistribute maximum-prefix 100 80`	Sets a maximum number of IP prefixes that are allowed to be redistributed into OSPF. • There is no default value for the *maximum* argument. • The *threshold* value defaults to 75 percent. **Note** If the **warning-only** keyword had been configured in this command, no limit would be enforced; a warning message is simply logged.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.
Step 7	**show ip ospf** [*process-id*] **Example:** `Router# show ip ospf 1`	(Optional) Displays general information about OSPF routing processes. • If a redistribution limit was configured, the output will include the maximum limit of redistributed prefixes and the threshold for warning messages.

Requesting a Warning About the Number of Routes Redistributed into OSPF

Note You cannot both limit redistributed prefixes and also choose to be warned.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
5. **redistribute maximum-prefix** *maximum* [*threshold*] **warning-only**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**redistribute** *protocol* [*process-id* | *as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match**{**internal**| **external 1**| **external 2**}][**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] **Example:** `Router(config-router)# redistribute eigrp 10`	Redistributes routes from one routing domain into another routing domain.
Step 5	**redistribute maximum-prefix** *maximum* [*threshold*] **warning-only** **Example:** `Router(config-router)# redistribute maximum-prefix 1000 80 warning-only`	Causes a warning message to be logged when the maximum number of IP prefixes has been redistributed into OSPF. • Because the **warning-only** keyword is included, no limit is imposed on the number of redistributed prefixes into OSPF. • There is no default value for the *maximum* argument. • The *threshold* value defaults to 75 percent. • 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

The following sections provide references related to the OSPF Limit on Number of Redistributed Routes feature.

Related Documents

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

Standards

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

MIBs

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

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for OSPF 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, page 130

Customizing OSPF LSA Throttling

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **timers throttle lsa all** *start-interval hold-interval max-interval*
5. **timers lsa arrival** *milliseconds*
6. **end**
7. **show ip ospf timers rate-limit**
8. **show ip ospf**

DETAILED STEPS

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process.
Step 4	**timers throttle lsa all** *start-interval hold-interval max-interval* **Example:** `Router(config-router)# timers throttle lsa all 100 10000 45000`	(Optional) Sets the rate-limiting values (in milliseconds) for LSA generation. • The default values are as follows: ◦ *start-interval*is 0 milliseconds. ◦ *hold-interval*is 5000 milliseconds. ◦ *max-interval*is 5000 milliseconds.
Step 5	**timers lsa arrival** *milliseconds* **Example:** `Router(config-router)# timers lsa arrival 2000`	(Optional) Sets the minimum interval (in milliseconds) between instances of receiving the same LSA. • The default value is 1000 milliseconds. • We suggest you keep the *milliseconds*value of the LSA arrival timer less than or equal to the neighbors' *hold-interval* value of the **timers throttle lsa all** command.
Step 6	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Command or Action	Purpose

Step 7 **show ip ospf timers rate-limit**
 	
Example:
 	
`Router#` **show ip ospf timers rate-limit**
 	
Example:
 	
Example:
 	
`LSAID: 10.1.1.1 Type: 1 Adv Rtr: 172.16.2.2 Due in: 00:00:00.028`
 	
Example:
 	
`LSAID: 192.168.4.1 Type: 3 Adv Rtr: 172.17.2.2 Due in: 00:00:00.028`
	(Optional) Displays a list of the LSAs in the rate limit queue (about to be generated).
	
	• The example shows two LSAs in the queue. Each LSA is identified by LSA ID number, Type (of LSA), Advertising router ID, and the time in hours:minutes:seconds (to the milliseconds) when the LSA is due to be generated.

Command or Action	Purpose

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`
	(Optional) Displays information about OSPF.
	• The output lines that specify initial throttle delay, minimum hold time for LSA throttle, and maximum wait time for LSA throttle indicate the LSA throttling values.

Command or Action	Purpose

Example:
`Initial LSA throttle delay 100 msecs`
Example:
`Minimum hold time for LSA throttle 10000 msecs`
Example:
`Maximum wait time for LSA throttle 45000 msecs`
Example:
`Minimum LSA arrival 1000 msecs`
Example:
`LSA group pacing timer 240 secs`
Example:
`Interface flood pacing timer 33 msecs`
Example:
`Retransmission pacing timer 66 msecs`
Example:
`Number of external LSA 0. Checksum Sum 0x0`
Example:
`Number of opaque AS LSA 0. Checksum Sum 0x0`
Example:
`Number of DCbitless external and opaque AS LSA 0`	

Command or Action	Purpose

Example:
`Number of DoNotAge external and opaque AS LSA 0`
Example:
`Number of areas in this router is 1. 1 normal 0 stub 0 nssa`
Example:
`External flood list length 0`
Example:
`Area 24`
Example:
`Number of interfaces in this area is 2`
Example:
`Area has no authentication`
Example:
`SPF algorithm last executed 04:28:18.396 ago`
Example:
`SPF algorithm executed 8 times`
Example:
`Area ranges are`
Example:
`Number of LSA 4. Checksum Sum 0x23EB9`	

Command or Action	Purpose

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"

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 12 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**

OSPF Support for Unlimited Software VRFs per PE Router

In a Multiprotocol Label Switching--Virtual Private Network (MPLS-VPN) deployment, each VPN routing and forwarding instance (VRF) needs a separate Open Shortest Path First (OSPF) process when configured to run OSPF. The OSPF Support for Unlimited Software VRFs per Provider Edge (PE) Router feature addresses the scalability issue for OSPF VPNs by eliminating the OSPF VPN limit of 32 processes.

Finding Feature Information

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

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

Prerequisites for OSPF Support for Unlimited Software VRFs per PE Router

You must have OSPF configured in your network.

Restrictions for OSPF Support for Unlimited Software VRFs per PE Router

Only 32 processes per VRF can be supported. For different VRF processes, there is no limit.

Information About OSPF Support for Unlimited Software VRFs per PE Router

Before Cisco IOS Releases 12.3(4)T and 12.0(27)S, a separate OSPF process was necessary for each VRF that receives VPN routes via OSPF. When VPNs are deployed, an MPLS Provider Edge (PE) router will be running both multiprotocol Border Gateway Protocol (BGP) for VPN distribution, and Interior Gateway Protocol (IGP) for PE-P connectivity. OSPF is commonly used as the IGP between a customer edge (CE) router and a PE router. OSPF was not scalable in a VPN deployment because of the limit of 32 processes. By default, one process is used for connected routes and another process is used for static routes; therefore only 28 processes can be created for VRFs.

The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature allows for an approximate range of 300 to 10,000 VRFs, depending on the particular platform and on the applications, processes, and protocols that are currently running on the platform.

How to Configure OSPF Support for Unlimited Software VRFs per PE Router

- Configuring Unlimited Software VRFs per PE Router, page 140

Configuring Unlimited Software VRFs per PE Router

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vpn-name* **Example:** `Router(config)# ip vrf crf-1`	Defines a VPN routing and forwarding (VRF) instance and enters VRP configuration mode.
Step 4	**exit** **Example:** `Router(config-vrf)# exit`	Returns to global configuration mode.
Step 5	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 1 vrf crf-1`	Enables OSPF routing. • The *process-id* argument identifies the OSPF process. • Use the **vrf** keyword and *vpn-name* argument to identify the VPN already defined in Step 3. **Note** You can now configure as many OSPF VRF processes as needed. Repeat Steps 3-5 as needed.
Step 6	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 7	**show ip ospf** [*process-id*] **Example:** `Router# show ip ospf 1`	Displays general information about OSPF routing processes.

Configuration Examples for OSPF Support for Unlimited Software VRFs per PE Router

Example Configuring OSPF Support for Unlimited Software VRFs per PE Router

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VRF processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf first
Router(config-vrf)# exit
Router(config)# ip vrf second
Router(config-vrf)# exit
Router(config)# ip vrf third
Router(config-vrf)# exit
Router(config)# router ospf 12 vrf first
Router(config-router)# exit
Router(config)# router ospf 13 vrf second
Router(config-router)# exit
Router(config)# router ospf 14 vrf third
Router(config)# end
```

Example Verifying OSPF Support for Unlimited Software VRFs per PE Router

This example illustrates the output from the **show ip ospf** command to verify that OSPF VRF process 12 has been created for the VRF named first. The output that relates to the VRF first appears in bold.

```
Router# show ip ospf 12
main ID type 0x0005, value 0.0.0.100
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Connected to MPLS VPN Superbackbone, VRF first
 It is an area border router
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x0
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
```

```
SPF algorithm last executed 00:00:15.204 ago
SPF algorithm executed 2 times
Area ranges are
Number of LSA 1. Checksum Sum 0xD9F3
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
```

Additional References

The following sections provide references related to the OSPF Support for Unlimited Software VRFs per Provider Edge Router feature.

Related Documents

Related Topic	Document Title
Configuring OSPF	"Configuring OSPF"

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPF Support for Unlimited Software VRFs per PE Router

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

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

Table 13 Feature Information for OSPF Support for Unlimited Software VRFs per Provider Edge Router

Feature Name	Releases	Feature Information
OSPF Support for Unlimited Software VRFs per Provider Edge Router	Cisco IOS XE Release 2.1	In a Multiprotocol Label Switching--Virtual Private Network (MPLS-VPN) deployment, each VPN routing and forwarding instance (VRF) needs a separate Open Shortest Path First (OSPF) process when configured to run OSPF. The OSPF Support for Unlimited Software VRFs per Provider Edge Router feature addresses the scalability issue for OSPF VPNs by eliminating the OSPF VPN limit of 32 processes.

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Information About OSPF Area Transit Capability

How the OSPF Area Transit Capability Feature Works

The OSPF Area Transit Capability feature is enabled by default. RFC 2328 defines OSPF area transit capability as the ability of the area to carry data traffic that neither originates nor terminates in the area itself. This capability enables the OSPF ABR to discover shorter paths through the transit area and to forward traffic along those paths rather than using the virtual link or path, which is not optimal.

For a detailed description of OSPF area transit capability, see RFC 2328, OSPF Version 2 .

How to Disable OSPF Area Transit Capability

Disabling OSPF Area Transit Capability on an Area Border Router

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vpn-name*]
4. **no capability transit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 100`	Enables OSPF routing and enters router configuration mode. • The *process-id* argument identifies the OSPF process.
Step 4	**no capability transit** **Example:** `Router(config-router)# no capability transit`	Disables OSPF area transit capability on all areas for a router process.

Additional References

The following sections provide references related to the OSPF Area Transit Capability feature.

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2328	OSPF Version 2

Technical Assistance

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

Feature Information for OSPF Area Transit Capability

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

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

Table 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**

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

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, page 152

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.

	Command or Action	Purpose
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.
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, page 153

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, page 153

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 15 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**

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 feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

Prerequisites for OSPF 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, page 161

Limiting the Number of Self-Generating LSAs for an OSPF Process

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **router-id** *ip-address*
5. **log -adjacency-changes** [**detail**]
6. **max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*]
7. **network** *ip-address wildcard-mask* **area** *area-id*
8. **end**
9. **show ip ospf** [*process-id area-id*] **database**[**database-summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Enables OSPF routing. • The *process-id* argument identifies the OSPF process.
Step 4	**router-id** *ip-address* **Example:** `Router(config-router)# router-id 10.0.0.1`	Specifies a fixed router ID for an OSPF process.

Command or Action	Purpose
Step 5 **log -adjacency-changes** [**detail**] **Example:** `Router(config-router)# log-adjacency-changes`	Configures the router to send a syslog message when an OSPF neighbor goes up or down.
Step 6 **max-lsa** *maximum-number* [*threshold-percentage*] [**warning-only**] [**ignore-time** *minutes*] [**ignore-count** *count-number*] [**reset-time** *minutes*] **Example:** `Router(config-router)# max-lsa 12000`	Limits the number of nonself-generated LSAs that an OSPF routing process can keep in the OSPF link-state database (LSDB).
Step 7 **network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Router(config-router)# network 209.165.201.1 255.255.255.255 area 0`	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.
Step 8 **end** **Example:** `Router(config-router)# end`	Ends the current configuration mode and returns to Privileged EXEC mode.
Step 9 **show ip ospf** [*process-id area-id*] **database**[**database-summary**] **Example:** `Router# show ip ospf 2000 database database-summary`	Displays lists of information related to the OSPF database for a specific router. • Use this command to verify the number of nonself-generated LSAs on a router.

Example

The **show ip ospf** command is entered with the **database-summary** keyword to verify the actual number of nonself-generated LSAs on a router. This command can be used at any time to display lists of information related to the OSPF database for a specific router.

```
Router# show ip ospf 2000 database database-summary

            OSPF Router with ID (192.168.1.3) (Process ID 2000)
Area 0 database summary
  LSA Type      Count    Delete   Maxage
  Router        5        0        0
  Network       2        0        0
  Summary Net   8        2        2
  Summary ASBR  0        0        0
  Type-7 Ext    0        0        0
    Prefixes redistributed in Type-7  0
```

```
  Opaque Link    0        0        0
  Opaque Area    0        0        0
  Subtotal       15       2        2
Process 2000 database summary
  LSA Type       Count    Delete   Maxage
  Router         5        0        0
  Network        2        0        0
  Summary Net    8        2        2
  Summary ASBR   0        0        0
  Type-7 Ext     0        0        0
  Opaque Link    0        0        0
  Opaque Area    0        0        0
  Type-5 Ext     4        0        0
    Prefixes redistributed in Type-5  0
  Opaque AS      0        0        0
  Non-self       16
  Total          19       2        2
```

Configuration Examples for OSPF Link-State Database Overload Protection

Setting a Limit for LSA Generation Example

In the following example, the router is configured to not accept any more nonself-generated LSAs once a maximum of 14,000 has been exceeded:

```
Router(config)# router ospf 1
Router(config-router)# router-id 192.168.0.1
Router(config-router)# log-adjacency-changes
Router(config-router)# max-lsa 14000
Router(config-router)# area 33 nssa
Router(config-router)# network 192.168.0.1 0.0.0.0 area 1
Router(config-router)# network 192.168.5.1 0.0.0.0 area 1
Router(config-router)# network 192.168.2.1 0.0.0.0 area 0
```

In the following example, the **show ip ospf** command has been entered to confirm the configuration:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 0
It is an area border and autonomous system boundary router
```

In the following example, the following output appears when the **show ip ospf** command has been entered during the time when the router is in the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
```

```
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1
   Ignoring all neighbors due to max-lsa limit, time remaining: 00:04:52
It is an area border and autonomous system boundary router
```

The following output appears when the **show ip ospf** command has been entered after the router left the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 1 - time remaining: 00:09:51
It is an area border and autonomous system boundary router
```

The following output appears when the **show ip ospf** command has been entered for a router that is permanently in the ignore state:

```
Router# show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Maximum number of non self-generated LSA allowed 14000
   Threshold for warning message 75%
   Ignore-time 5 minutes, reset-time 10 minutes
   Ignore-count allowed 5, current ignore-count 6
   Permanently ignoring all neighbors due to max-lsa limit
It is an area border and autonomous system boundary router
```

Additional References

The following sections provide references related to the OSPF Link-State Database Overload Protection feature.

Related Documents

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

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPF Link-State Database Overload Protection

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

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

Table 16 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**

OSPF MIB Support of RFC 1850 and Latest Extensions

The OSPF MIB Support of RFC 1850 and Latest Extensions feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring on the Open Shortest Path First (OSPF) routing protocol. Users have an improved ability to constantly monitor the changing state of an OSPF network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes. The protocol information collected by the OSPF MIB objects and trap objects can be used to derive statistics that will help monitor and improve overall network performance.

Finding Feature Information

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

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

Prerequisites for OSPF MIB Support of RFC 1850 and Latest Extensions

- OSPF must be configured on the router.
- Simple Network Management Protocol (SNMP) must be enabled on the router before notifications (traps) can be configured or before SNMP GET operations can be performed.

Information About OSPF MIB Support of RFC 1850 and Latest Extensions

The following sections contain information about MIB objects standardized as part of RFC 1850 and defined in OSPF-MIB and OSPF-TRAP-MIB. In addition, extensions to RFC 1850 objects are described as defined in the two Cisco private MIBs, CISCO-OSPF-MIB and CISCO-OSPF-TRAP-MIB.

OSPF MIB Changes to Support RFC 1850

OSPF MIB

This section describes the new MIB objects that are provided by RFC 1850 definitions. These OSPF MIB definitions provide additional capacity that is not provided by the standard OSPF MIB that supported the previous RFC 1253. To see a complete set of OSPF MIB objects, see the OSPF-MIB file.

The table below shows the new OSPF-MIB objects that are provided by RFC 1850 definitions. The objects are listed in the order in which they appear within the OSPF-MIB file, per the tables that describe them.

Table 17 New OSPF-MIB Objects

OSPF-MIB Table	New MIB Objects
OspfAreaEntry table	• OspfAreaSummary • OspfAreaStatus
OspfStubAreaEntry	• OspfStubMetricType
OspfAreaRangeEntry	• OspfAreaRangeEffect
OspfHostEntry	• OspfHostAreaID
OspfIfEntry	• OspfIfStatus • OspfIfMulticastForwarding • OspfIfDemand • OspfIfAuthType
OspfVirtIfEntry	• OspfVirtIfAuthType

OSPF-MIB Table	New MIB Objects
OspfNbrEntry	• OspfNbmaNbrPermanence • OspfNbrHelloSuppressed
OspfVirtNbrEntry	• OspfVirtNbrHelloSuppressed
OspfExtLsdbEntry	• OspfExtLsdbType • OspfExtLsdbLsid • OspfExtLsdbRouterId • OspfExtLsdbSequence • OspfExtLsdbAge • OspfExtLsdbChecksum • OspfExtLsdbAdvertisement
OspfAreaAggregateEntry	• OspfAreaAggregateAreaID • OspfAreaAggregateLsdbType • OspfAreaAggregateNet • OspfAreaAggregateMask • OspfAreaAggregateStatusospfSetTrap • OspfAreaAggregateEffect

OSPF TRAP MIB

This section describes scalar objects and MIB objects that are provided to support RFC 1850.

The following scalar objects are added to OSPF-TRAP-MIB and are listed in the order in which they appear in the OSPF-TRAP-MIB file:

- OspfExtLsdbLimit
- OspfMulticastExtensions
- OspfExitOverflowInterval
- OspfDemandExtensions

The ospfSetTrap control MIB object contains the OSPF trap MIB objects that enable and disable OSPF traps in the IOS CLI. These OSPF trap MIB objects are provided by the RFC 1850 standard OSPF MIB. To learn how to enable and disable the OSPF traps, see the How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, page 173.

The table below shows the OSPF trap MIB objects, listed in the order in which they appear within the OSPF-TRAP-MIB file.

Table 18 New OSPF-TRAP-MIB Objects

OSPF Control MIB Object	Trap MIB Objects
ospfSetTrap	• ospfIfStateChange • ospfVirtIfStateChange • ospfNbrStateChange • ospfVirtNbrState • ospfIfConfigError • ospfVirtIfConfigError • ospfIfAuthFailure • ospfVirtIfAuthFailure • ospfIfRxBadPacket • ospfVirtIfRxBadPacket • ospfTxRetransmit • ospfVirtIfTxRetransmit • ospfOriginateLsa • ospfMaxAgeLsa

CISCO OSPF MIB

This section describes scalar and Cisco-specific OSPF MIB objects that are provided as extensions to support the RFC 1850 OSPF MIB definitions, to provide capability that the standard MIB cannot provide.

The following scalar objects are added to OSPF-OSPF-MIB:

- cospfRFC1583Compatibility
- cospfOpaqueLsaSupport
- cospfOpaqueASLsaCount
- cospfOpaqueASLsaCksumSum

For each of the following table entries, the new Cisco-specific MIB objects that are provided as extensions to support the RFC 1850 OSPF MIB definitions are listed. To see the complete set of objects for the Cisco-specific OSPF MIB, refer to the CISCO-OSPF-MIB file.

The table below shows the new CISCO-OSPF-MIB objects that are provided by RFC 1850 definitions. The objects are listed in the order in which they appear within the CISCO-OSPF-MIB file, per the tables that describe them.

Table 19 New CISCO-OSPF-MIB Objects

CISCO-OSPF-MIB Table	New MIB Objects
cospfAreaEntry	• cospfOpaqueAreaLsaCount • cospfOpaqueAreaLsaCksumSum • cospfAreaNssaTranslatorRole • cospfAreaNssaTranslatorState • cospfAreaNssaTranslatorEvents

CISCO-OSPF-MIB Table	New MIB Objects
cospfLsdbEntry	• cospfLsdbType • cospfLsdbSequence • cospfLsdbAge • cospfLsdbChecksum • cospfLsdbAdvertisement
cospfIfEntry	• cospfIfLsaCount • cospfIfLsaCksumSum
cospfVirtIfEntry	• cospfVirtIfLsaCount • cospfVirtIfLsaCksumSum
cospfLocalLsdbEntry	• cospfLocalLsdbIpAddress • cospfLocalLsdbAddressLessIf • cospfLocalLsdbType • cospfLocalLsdbLsid • cospfLocalLsdbRouterId • cospfLocalLsdbSequence • cospfLocalLsdbAge • cospfLocalLsdbChecksum • cospfLocalLsdbAdvertisement
cospfVirtLocalLsdbEntry	• cospfVirtLocalLsdbTransitArea • cospfVirtLocalLsdbNeighbor • cospfVirtLocalLsdbType • cospfVirtLocalLsdbLsid • cospfVirtLocalLsdbRouterId • cospfVirtLocalLsdbSequence • cospfVirtLocalLsdbAge • cospfVirtLocalLsdbChecksum • cospfVirtLocalLsdbAdvertisement

CISCO OSPF TRAP MIB

The cospfSetTrap MIB object represents trap events in CISCO-OSPF-TRAP-MIB. This is a bit map, where the first bit represents the first trap. The following MIB objects are TRAP events that have been added to support RFC 1850. To see a complete set of Cisco OSPF Trap MIB objects, see the CISCO-OSPF-TRAP-MIB file.

The table below shows the trap events described within the cospfSetTrap MIB object in the CISCO-TRAP-MIB:

Table 20 CISCO-OSPF Trap Events

CISCO-OSPF-TRAP-MIB Trap Events	Trap Event Description
cospfIfConfigError	This trap is generated for mismatched MTU parameter errors that occur when nonvirtual OSPF neighbors are forming adjacencies.
cospfVirtIfConfigError	This trap is generated for mismatched MTU parameter errors when virtual OSPF neighbors are forming adjacencies.
cospfTxRetransmit	This trap is generated in the case of opaque LSAs when packets are sent by a nonvirtual interface. An opaque link-state advertisement (LSA) is used in MPLS traffic engineering to distribute attributes such as capacity and topology of links in a network. The scope of this LSA can be confined to the local network (Type 9, Link-Local), OSPF area (Type 20, Area-Local), or autonomous system (Type 11, AS scope). The information in an opaque LSA can be used by an external application across the OSPF network.
cospfVirtIfTxRetransmit	This trap is generated in the case of opaque LSAs when packets are sent by a virtual interface.
cospfOriginateLsa	This trap is generated when a new opaque LSA is originated by the router when a topology change has occurred.
cospfMaxAgeLsa	The trap is generated in the case of opaque LSAs.
cospfNssaTranslatorStatusChange	The trap is generated if there is a change in the ability of a router to translate OSPF type-7 LSAs into OSPF type-5 LSAs.

For information about how to enable OSPF MIB traps, see the How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, page 173.

Benefits of the OSPF MIB

The OSPF MIBs (OSPF-MIB and OSPF-TRAP-MIB) and Cisco private OSPF MIBs (CISCO-OSPF-MIB and CISCO-OSPF-TRAP-MIB) allow network managers to more effectively monitor the OSPF routing protocol through the addition of new table objects and trap notification objects that previously were not supported by the RFC 1253 OSPF MIB.

New CLI commands have been added to enable SNMP notifications for OSPF MIB support objects, Cisco-specific errors, retransmission and state-change traps. The SNMP notifications are provided for errors and other significant event information for the OSPF network.

How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions

Enabling OSPF MIB Support

Before the OSPF MIB Support of RFC 1850 and Latest Extensions feature can be used, the SNMP server for the router must be configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string1* **ro**
4. **snmp-server community** *string2* **rw**
5. **snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
6. **snmp-server enable traps ospf**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server community** *string1* **ro** **Example:** `Router(config)# snmp-server community public ro`	Enables read access to all objects in the MIB, but does not allow access to the community strings.

	Command or Action	Purpose
Step 4	**snmp-server community** *string2* **rw** **Example:** `Router(config)# snmp-server community private rw`	Enables read and write access to all objects in the MIB, but does not allow access to the community strings.
Step 5	**snmp-server host** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Router(config)# snmp-server host 172.20.2.162 version 2c public ospf`	Specifies a recipient (target host) for SNMP notification operations. • If no *notification-type* is specified, all enabled notifications (traps or informs) will be sent to the specified host. • If you want to send only the OSPF notifications to the specified host, you can use the optional **ospf**keyword as one of the *notification-types*. (See the example.) Entering the **ospf** keyword enables the ospfSetTrap trap control MIB object.
Step 6	**snmp-server enable traps ospf** **Example:** `Router(config)# snmp-server enable traps ospf`	Enables all SNMP notifications defined in the OSPF MIBs. **Note** This step is required only if you wish to enable all OSPF traps. When you enter the **no snmp-server enable traps ospf** command, all OSPF traps will be disabled.
Step 7	**end** **Example:** `Router(config)# end`	Ends your configuration session and exits global configuration mode.

• What to Do Next, page 174

What to Do Next

If you did not want to enable all OSPF traps, follow the steps in the following section to selectively enable one or more types of OSPF trap:

Enabling Specific OSPF Traps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ospf cisco-specific errors** [**config-error**] [**virt-config-error**]
4. **snmp-server enable traps ospf cisco-specific retransmit** [**packets**] [**virt-packets**]
5. **snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change**] [**shamlink-state-change**]
6. **snmp-server enable traps ospf cisco-specific lsa** [**lsa-maxage**] [**lsa-originate**]
7. **snmp-server enable traps ospf errors** [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**]
8. **snmp-server enable traps ospf lsa** [**lsa-maxage**] [**lsa-originate**]
9. **snmp-server enable traps ospf rate-limit** *seconds trap-number*
10. **snmp-server enable traps ospf retransmit** [**packets**] [**virt-packets**]
11. **snmp-server enable traps ospf state-change** [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server enable traps ospf cisco-specific errors** [**config-error**] [**virt-config-error**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific errors config-error`	Enables SNMP notifications for Cisco-specific OSPF configuration mismatch errors. • Entering the **snmp-server enable traps ospf cisco-specific errors** command with the optional **virt-config-error** keyword enables only the SNMP notifications for configuration mismatch errors on virtual interfaces.

	Command or Action	Purpose
Step 4	**snmp-server enable traps ospf cisco-specific retransmit** [**packets**] [**virt-packets**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific retransmit packets virt-packets`	Enables error traps for Cisco-specific OSPF errors that involve re-sent packets. • Entering the **snmp-server enable traps ospf cisco-specific retransmit** command with the optional **virt-packets**keyword enables only the SNMP notifications for packets that are re-sent on virtual interfaces.
Step 5	**snmp-server enable traps ospf cisco-specific state-change** [**nssa-trans-change**] [**shamlink-state-change**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific state-change`	Enables all error traps for Cisco-specific OSPF transition state changes.
Step 6	**snmp-server enable traps ospf cisco-specific lsa** [**lsa-maxage**] [**lsa-originate**] **Example:** `Router(config)# snmp-server enable traps ospf cisco-specific lsa`	Enables error traps for opaque LSAs.
Step 7	**snmp-server enable traps ospf errors** [**authentication-failure**] [**bad-packet**] [**config-error**] [**virt-authentication-failure**] [**virt-config-error**] **Example:** `Router(config)# snmp-server enable traps ospf errors virt-config-error`	Enables error traps for OSPF configuration errors. • Entering the **snmp-server enable traps ospf errors** command with the optional **virt-config-error**keyword enables only the SNMP notifications for OSPF configuration errors on virtual interfaces.
Step 8	**snmp-server enable traps ospf lsa** [**lsa-maxage**] [**lsa-originate**] **Example:** `Router(config)# snmp-server enable traps ospf lsa`	Enables error traps for OSPF LSA errors.
Step 9	**snmp-server enable traps ospf rate-limit** *seconds trap-number* **Example:** `Router(config)# snmp-server enable traps ospf rate-limit 20 20`	Sets the rate limit for how many SNMP OSPF notifications are sent in each OSPF SNMP notification rate-limit window.

	Command or Action	Purpose
Step 10	**snmp-server enable traps ospf retransmit** [**packets**] [**virt-packets**] **Example:** `Router(config)# snmp-server enable traps ospf retransmit`	Enables SNMP OSPF notifications for re-sent packets.
Step 11	**snmp-server enable traps ospf state-change** [**if-state-change**] [**neighbor-state-change**] [**virtif-state-change**] [**virtneighbor-state-change**] **Example:** `Router(config)# snmp-server enable traps ospf state-change`	Enables SNMP OSPF notifications for OSPF transition state changes.

Verifying OSPF MIB Traps on the Router

SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** [*options*] **Example:** `Router# show running-config | include traps`	Displays the contents of the currently running configuration file and includes information about enabled traps. • Verifies which traps are enabled.

Configuration Examples for OSPF MIB Support of RFC 1850 and Latest Extensions

Example Enabling and Verifying OSPF MIB Support Traps

The following example enables all OSPF traps.

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" chapter of the Cisco IOS XE Network Management Configuration Guide, *Release 2* .

Additional References

The following sections provide references related to the OSPF MIB Support of RFC 1850 and Latest Extensions feature.

Related Documents

Related Topic	Document Title
SNMP commands	*Cisco IOS Network Management Command Reference*
Configuring OSPF	"Configuring OSPF"
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

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

MIB

MIB	MIBs Link
• CISCO-OSPF-MIB • CISCO-OSPF-TRAP-MIB • OSPF-MIB • OSPF-TRAP-MIB	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

RFC

RFC	Title
RFC 1850	*OSPF MIB Support*

Technical Assistance

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

Feature Information for OSPF MIB Support of RFC 1850 and Latest Extensions

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

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

Table 21 Feature Information for OSPF MIB Support of RFC 1850 and Latest Extensions

Feature Name	Releases	Feature Information
OSPF MIB Support of RFC 1850 and Latest Extensions	Cisco IOS XE Release 2.1	The OSPF MIB Support of RFC 1850 and Latest Extensions feature introduces the capability for Simple Network Management Protocol (SNMP) monitoring on the Open Shortest Path First (OSPF) routing protocol. Users have an improved ability to constantly monitor the changing state of an OSPF network by use of MIB objects to gather information relating to protocol parameters and trap notification objects that can signal the occurrence of significant network events such as transition state changes. The protocol information collected by the OSPF MIB objects and trap objects can be used to derive statistics that will help monitor and improve overall network performance. The following commands are introduced or modified in the feature documented in this module: • **snmp-server enable traps ospf** • **snmp-server enable traps ospf cisco-specific errors** • **snmp-server enable traps ospf cisco-specific lsa** • **snmp-server enable traps ospf cisco-specific retransmit** • **snmp-server enable traps ospf cisco-specific state-change** • **snmp-server enable traps ospf errors** • **snmp-server enable traps ospf lsa** • **snmp-server enable traps ospf rate-limit**

Feature Name	Releases	Feature Information
		• **snmp-server enable traps ospf retransmit** • **snmp-server enable traps ospf state-change**

OSPF Enhanced Traffic Statistics

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

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

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

Finding Feature Information

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

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

Prerequisites for OSPF Enhanced Traffic Statistics

OSPFv2 or OSPFv3 must be configured on the router.

Information About OSPF Enhanced Traffic Statistics

The OSPF enhanced traffic statistics are enabled by default and cannot be disabled.

The detailed OSPF traffic statistics are especially beneficial for troubleshooting the following types of OSPF instabilities:

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

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

How to Display and Clear OSPF Enhanced Traffic Statistics

Displaying and Clearing OSPF Traffic Statistics for OSPFv2

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ip ospf 10 traffic gigabitethernet 0/0/0`	Displays OSPFv2 traffic statistics.
Step 3	**clear ip ospf traffic** **Example:** `Router# clear ip ospf traffic`	Clears OSPFv2 traffic statistics.

Displaying and Clearing OSPF Traffic Statistics for OSPFv3

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ipv6 ospf** [*process-id*] **traffic**[*interface-type interface-number*] **Example:** `Router# show ipv6 ospf traffic`	Displays OSPFv3 traffic statistics.
Step 3	**clear ipv6 ospf traffic** **Example:** `Router# clear ipv6 ospf traffic`	Clears OSPFv3 traffic statistics.

Configuration Examples for OSPF Enhanced Traffic Statistics

Example Displaying and Clearing Enhanced Traffic Statistics for OSPFv2

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

```
Router# show ip ospf traffic
OSPF statistics:
 Rcvd: 55 total, 0 checksum errors
       22 hello, 7 database desc, 2 link state req
       6 link state updates, 6 link state acks
  Sent: 68 total
       45 hello, 7 database desc, 2 link state req
       10 link state updates, 4 link state acks
           OSPF Router with ID (10.1.1.1) (Process ID 8)
OSPF queues statistic for process ID 8:
```

```
  OSPF Hello queue size 0, no limit, drops 0, max size 0
  OSPF Router queue size 0, limit 200, drops 0, max size 0
Interface statistics:
    Interface GigabitEthernet0/0/1
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0
  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 8:
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      0                    0
  RX DB des     0                    0
  RX LS req     0                    0
  RX LS upd     0                    0
  RX LS ack     0                    0
  RX Total      0                    0
  TX Failed     0                    0
  TX Hello      16                   1216
  TX DB des     0                    0
  TX LS req     0                    0
  TX LS upd     0                    0
  TX LS ack     0                    0
  TX Total      16                   1216
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
           OSPF Router with ID (10.1.1.4) (Process ID 1)
OSPF queues statistic for process ID 1:
  OSPF Hello queue size 0, no limit, drops 0, max size 2
  OSPF Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0/0
OSPF packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      11                   528
  RX DB des     4                    148
  RX LS req     1                    60
  RX LS upd     3                    216
  RX LS ack     2                    128
  RX Total      21                   1080
  TX Failed     0                    0
 TX Hello      14                   1104
  TX DB des     3                    252
  TX LS req     1                    56
  TX LS upd     3                    392
```

```
  TX LS ack     2                   128
  TX Total      23                  1932
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 0,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
    Interface GigabitEthernet0/0/0
OSPF packets received/sent
  Type          Packets             Bytes
  RX Invalid    0                   0
  RX Hello      13                  620
  RX DB des     3                   116
  RX LS req     1                   36
  RX LS upd     3                   228
  RX LS ack     4                   216
  RX Total      24                  1216
  TX Failed     0                   0
  TX Hello      17                  1344
  TX DB des     4                   276
  TX LS req     1                   56
  TX LS upd     7                   656
  TX LS ack     2                   128
  TX Total      31                  2460
OSPF header errors
  Length 0, Checksum 0, Version 0, Bad Source 13,
  No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
  Self Originated 0, Duplicate ID 0, Hello 0,
  MTU Mismatch 0, Nbr Ignored 0, LLS 0,
  Authentication 0,
OSPF LSA errors
  Type 0, Length 0, Data 0, Checksum 0,

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

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

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

Example Displaying and Clearing Enhanced Traffic Statistics for OSPFv3

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

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
  Rcvd: 32 total, 0 checksum errors
        10 hello, 7 database desc, 2 link state req
        9 link state updates, 4 link state acks
        0 LSA ignored
  Sent: 45 total, 0 failed
        17 hello, 12 database desc, 2 link state req
        8 link state updates, 6 link state acks
            OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
  Hello queue size 0, no limit, max size 2
  Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
    Interface Serial2/0/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      5                    196
  RX DB des     4                    172
  RX LS req     1                    52
  RX LS upd     4                    320
  RX LS ack     2                    112
  RX Total      16                   852
  TX Failed     0                    0
  TX Hello      8                    304
  TX DB des     3                    144
  TX LS req     1                    52
  TX LS upd     3                    252
  TX LS ack     3                    148
  TX Total      18                   900
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Interface GigabitEthernet0/0/0
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid    0                    0
  RX Hello      6                    240
  RX DB des     3                    144
  RX LS req     1                    52
  RX LS upd     5                    372
  RX LS ack     2                    152
  RX Total      17                   960
  TX Failed     0                    0
  TX Hello      11                   420
  TX DB des     9                    312
  TX LS req     1                    52
  TX LS upd     5                    376
  TX LS ack     3                    148
  TX Total      29                   1308
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
Summary traffic statistics for process ID 6:
OSPFv3 packets received/sent
  Type          Packets              Bytes
```

```
  RX Invalid    0                   0
  RX Hello      11                  436
  RX DB des     7                   316
  RX LS req     2                   104
  RX LS upd     9                   692
  RX LS ack     4                   264
  RX Total      33                  1812
  TX Failed     0                   0
  TX Hello      19                  724
  TX DB des     12                  456
  TX LS req     2                   104
  TX LS upd     8                   628
  TX LS ack     6                   296
  TX Total      47                  2208
OSPFv3 header errors
  Length 0, Checksum 0, Version 0, No Virtual Link 0,
  Area Mismatch 0, Self Originated 0, Duplicate ID 0,
  Instance ID 0, Hello 0, MTU Mismatch 0,
  Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
  Type 0, Length 0, Data 0, Checksum 0,
```

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
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 Enhanced Traffic Statistics

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

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

Table 22 Feature Information for OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

Feature Name	Releases	Feature Information
OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3	Cisco IOS XE Release 2.1	This document describes the detailed OSPF traffic statistics that are provided when the user enters the new and modified show commands for OSPFv2 and OSPFv3. The following commands are introduced or modified in the feature documented in this module: • **clear ipv6 ospf traffic** • **show ip ospf traffic** • **show ipv6 ospf traffic**

Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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

Finding Feature Information

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

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

Information About OSPF TTL Security Check and OSPF Graceful Shutdown

TTL Security Check for OSPF

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

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

Transitioning Existing Networks to Use TTL Security Check

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

TTL Security Check for OSPF Virtual and Sham Links

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a *virtual link*. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other area border router [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. Sham links are similar to virtual links in many ways, but sham links are used in Layer 3 Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) networks to connect Provider Edge (PE) routers across the MPLS backbone.

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

Benefits of the OSPF Support for TTL Security Check

The OSPF Support for TTL Security Check feature provides an effective and easy-to-deploy solution to protect OSPF neighbor sessions from CPU utilization-based attacks. When this feature is enabled, a host cannot attack an OSPF session if the host is not a member of the local or remote OSPF network, or if the host is not directly connected to a network segment between the local and remote OSPF networks. This solution greatly reduces the effectiveness of Denial of Service (DoS) attacks against an OSPF autonomous system.

OSPF Graceful Shutdown

The OSPF Graceful Shutdown feature provides the ability to temporarily shut down the OSPF protocol in the least disruptive manner and notify its neighbors that it is going away. All traffic that has another path

through the network will be directed to that alternate path. A graceful shutdown of the OSPF protocol can be initiated using the **shutdown** command in router configuration mode.

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

How to Configure OSPF TTL Security Check and OSPF Graceful Shutdown

Configuring TTL Security Check on All OSPF Interfaces

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuring TTL Security Check on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

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

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

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

Configuring OSPF Graceful Shutdown on a Per-Interface Basis

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Examples for OSPF TTL Security Check and OSPF Graceful Shutdown

• Example: Transitioning an Existing Network to Use TTL Security Check, page 200

Example: Transitioning an Existing Network to Use TTL Security Check

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

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

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

Technical Assistance

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

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

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

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

Table 23 Feature Information for Configuring OSPF TTL Security Check and OSPF Graceful Shutdown

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

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

OSPF Sham-Link MIB Support

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

Finding Feature Information

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

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

Prerequisites for OSPF Sham-Link MIB Support

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

Restrictions for OSPF Sham-Link MIB Support

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

Information About OSPF Sham-Link MIB Support

OSPF Sham-Links in PE-PE Router Connections

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

Cisco OSPF MIB and Cisco OSPF Trap MIB Enhancements

The OSPF Sham-Link MIB Support feature introduces MIB support for OSPF sham-links through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New command-line interface (CLI) commands have been added to enable SNMP notifications for the OSPF sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface.

OSPF Sham-Link Configuration Support

The cospfShamLinksTable table object stores information about the sham-links that have been configured for the OSPF area. The cospfShamLinksTable allows access to the following MIB objects:

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

OSPF Sham-Link Neighbor Support

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

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

OSPF Sham-Link Interface Transition State Change Support

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

- ospfRouterId
- cospfShamLinksAreaId
- cospfShamLinksLocalIpAddrType
- cospfShamLinksLocalIpAddr
- cospfShamLinksRemoteIpAddrType
- cospfShamLinksRemoteIpAddr
- cospfShamLinksState

OSPF Sham-Link Neighbor Transition State Change Support

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

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

Sham-Link Errors

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

- cospfShamLinkConfigError

- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

How to Configure OSPF Sham-Link MIB Support

Configuring the Router to Enable Sending of SNMP Notifications

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** **Example:** `Router# show running-config`	Displays the running configuration to determine if an SNMP agent is already running. • If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.
Step 3	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

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

Enabling Sending of OSPF Sham-Link Error Traps

SUMMARY STEPS

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

DETAILED STEPS

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

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

Enabling OSPF Sham-Link Retransmissions Traps

SUMMARY STEPS

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

DETAILED STEPS

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

Enabling OSPF Sham-Link State Change Traps

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

SUMMARY STEPS

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

DETAILED STEPS

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

Verifying OSPF Sham-Link MIB Traps on the Router

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show running-config** | **include traps** **Example:** `Router# show running-config | include traps`	Displays the contents of the currently running configuration file and includes information about enabled traps. • Verifies if the trap is enabled.

Configuration Examples for OSPF Sham-Link MIB Support

Example Enabling and Verifying OSPF Sham-Link Error Traps

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

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

% Sham-link config error trap not enabled.
% Configure "cisco-specific errors config-error" first.
% This requirement allows both traps to be sent.
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
Router(config)# end
```

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific errors config-error
snmp-server enable traps ospf cisco-specific errors shamlink
```

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

```
Router# configure terminal
```

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

Example Enabling and Verifying OSPF State Change Traps

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

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
```

Note that the **snmp-server enable traps ospf cisco-specific state-change shamlink** command enables the sham-link interface state change for the cospfShamLinksStateChange trap.

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

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

Example Enabling and Verifying OSPF Sham-Link Retransmissions Traps

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

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

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

```
Router# show running-config | include traps
snmp-server enable traps ospf cisco-specific retransmit shamlink
```

Where to Go Next

For more information about SNMP and SNMP operations, see the "Configuring SNMP Support" part of the *Cisco IOS XE Network Management Configuration Guide, Release 2* .

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for OSPF Sham-Link MIB Support

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

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

Table 24 Feature Information for OSPF Sham-Link MIB Support

Feature Name	Releases	Feature Information
OSPF Sham-Link MIB Support	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	This feature introduces MIB support for the OSPF Sham-Link feature through the addition of new tables and trap MIB objects to the Cisco OSPF MIB (CISCO-OSPF-MIB) and to the Cisco OSPF Trap MIB (CISCO-OSPF-TRAP-MIB). New commands have been added to enable Simple Network Management Protocol (SNMP) notifications for the Open Shortest Path First (OSPF) sham-link trap objects. Notifications are provided for errors, state changes, and retransmissions across a sham-link interface. The following commands are introduced or modified in the feature documented in this module: • **snmp-server enable traps ospf cisco-specific errors config-error** • **snmp-server enable traps ospf cisco-specific errors shamlink** • **snmp-server enable traps ospf cisco-specific retransmit** • **snmp-server enable traps ospf cisco-specific state-change.**

OSPF SNMP ifIndex Value for Interface ID in Data Fields

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

Finding Feature Information

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

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

Prerequisites for SNMP ifIndex Value for Interface ID in Data Fields

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

Information About SNMP ifIndex Value for Interface ID in Data Fields

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

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

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

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

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

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

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

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

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

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

Configuring OSPF interfaces to use SNMP MIB-II ifIndex Numbers

SUMMARY STEPS

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

DETAILED STEPS

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

	Command or Action	Purpose

Step 3	Do one of the following:
	• **router ospf** *process-id* [**vrf** *vpn-name*]
	•
	• **ipv6 router ospf** *process-id*
	Example:
	`Router(config)# router ospf 4`
	Example:
	Example:
	`Router(config)# ipv6 router ospf 4`
		Configures an OSPFv2 routing process and enters router configuration mode.
		Configures an OSPFv3 routing process and enters router configuration mode.
		Note If you configure an OSPFv3 routing process, that uses IPv6, you must have already enabled IPv6.

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

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

- Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2, page 223
- Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3, page 223

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv2

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

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

Serial13/0: Ifindex = 53
```

Example Configuring SNMP ifIndex Value for Interface ID for OSPFv3

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

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

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

```
Router# show snmp mib ifmib ifindex GigabitEthernet 0/0/0
0/0/0: Ifindex = 5
Router# show ipv6 ospf interface
OSPF_VL0 is up, line protocol is up
  Interface ID 71
  Area 0, Process ID 1, Instance ID 0, Router ID 172.16.0.1
  Network Type VIRTUAL_LINK, Cost: 10
  Configured as demand circuit.
  Run as demand circuit.
  DoNotAge LSA allowed.
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 1/2/3, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
```

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

```
  Checksum: 0xB6E7
  Length: 52
  Referenced LSA Type: 2001
  Referenced Link State ID: 0
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:2:0:A8BB:CCFF:FE00:6F02
  Prefix Length: 128, Options: LA , Metric: 0
  Routing Bit Set on this LSA
  LS age: 151
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 1006
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000001
  Checksum: 0x6E24
  Length: 44
  Referenced LSA Type: 2002
  Referenced Link State ID: 6
  Referenced Advertising Router: 172.16.0.1
  Number of Prefixes: 1
  Prefix Address: 2002:0:1::
  Prefix Length: 64, Options: None, Metric: 0
Router# show ipv6 ospf database router

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

```
Neighbor (DR) Router ID: 172.16.0.1
LS age: 175
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Router Links
Link State ID: 0
Advertising Router: 172.16.0.1
LS Seq Number: 80000004
Checksum: 0xBD10
Length: 40
Area Border Router
Number of Links: 1
    Link connected to: a Transit Network
Link Metric: 10
Local Interface ID: 6
Neighbor (DR) Interface ID: 6
Neighbor (DR) Router ID: 172.16.0.1
Router# show ipv6 ospf database link adv-router 172.16.0.1
OSPFv3 Router with ID (172.16.0.1) (Process ID 1)
Link (Type-8) Link States (Area 0)
  LS age: 245
  Options: (V6-Bit E-Bit R-bit DC-Bit)
  LS Type: Link-LSA (Interface: GigabitEthernet2/0)
  Link State ID: 10 (Interface ID)
  Advertising Router: 172.16.0.1
  LS Seq Number: 80000002
  Checksum: 0xA0CB
  Length: 56
  Router Priority: 1
  Link Local Address: FE80::A8BB:CCFF:FE00:6F02
  Number of Prefixes: 1
  Prefix Address: 2002:0:2::
  Prefix Length: 64, Options: None
Link (Type-8) Link States (Area 1)
LS age: 250
Options: (V6-Bit E-Bit R-bit DC-Bit)
LS Type: Link-LSA (Interface: GigabitEthernet1/0)
Link State ID: 6 (Interface ID)
Advertising Router: 172.16.0.1
LS Seq Number: 80000001
Checksum: 0x4F94
Length: 44
Router Priority: 1
Link Local Address: FE80::A8BB:CCFF:FE00:6F01
Number of Prefixes: 0
```

Additional References

The following sections provide references related to the OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields feature.

Related Documents

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

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS XE software 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 2740	*OSPF Version 3*

Technical Assistance

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

Feature Information for OSPF SNMP ifIndex Value for Interface ID

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

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

Table 25 Feature Information for OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields

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

OSPFv2 Local RIB

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

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

Finding Feature Information

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

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

Prerequisites for OSPFv2 Local RIB

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

Restrictions for OSPFv2 Local RIB

This feature is available only for IP Version 4 networks.

Information About OSPFv2 Local RIB

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

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

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

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

How to Configure OSPFv2 Local RIB

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

- Changing the Default Local RIB Criteria, page 230
- Changing the Administrative Distance for Discard Routes, page 232

Changing the Default Local RIB Criteria

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**local-rib-criteria** [**forwarding-address**] [**inter-area-summary**] [**nssa-translation**] **Example:** `Router(config-router)# local-rib-criteria forwarding-address`	Specifies that the OSPF local RIB will be used for route validation.
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip ospf** *process-id* **rib** [**redistribution**] [*network-prefix*] [*network-mask*] [**detail**] **Example:** `Router# show ip ospf 23 rib`	Displays information for the OSPF local RIB or locally redistributed routes.

Changing the Administrative Distance for Discard Routes

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* [**vrf** *vpn-name*] **Example:** `Router(config)# router ospf 23`	Configures an OSPFv2 routing process and enters router configuration mode.
Step 4	**discard-route** [**external** [*distance*]] [**internal** [*distance*]] **Example:** `Router(config-router)# discard-route external 150`	Reinstalls either an external or internal discard route that was previously removed. **Note** You can now specify the administrative distance for internal and external discard routes.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-router)# end`	Returns to privileged EXEC mode.
Step 6	**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**] **Example:** `Router# show ip route ospf 23`	Displays the current state of the routing table. **Note** Entering the **show ip route** command will verify the changed administrative distance values for external and internal discard routes.

Example

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

```
Router# show ip route 192.168.0.0 255.255.255.0

Routing entry for 192.168.0.0/24

      Known via "ospf 1", distance 110, metric 0, type intra area

  Routing Descriptor Blocks:

  * directly connected, via Null0

       Route metric is 0, traffic share count is 1
```

- Troubleshooting Tips, page 233

Troubleshooting Tips

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

Configuration Examples for OSPFv2 Local RIB

- Example: Changing the Default Local RIB Criteria, page 234
- Example: Changing the Administrative Distance for Discard Routes, page 234

Example: Changing the Default Local RIB Criteria

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

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

Example: Changing the Administrative Distance for Discard Routes

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

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

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

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

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

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

Additional References

The following sections provide references related to OSPFv2 Local RIB.

Related Documents

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

Related Topic	Document Title
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
None	--

Technical Assistance

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

Feature Information for OSPFv2 Local RIB

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

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

Table 26 Feature Information for the OSPFv2 Local RIB

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

OSPF Support for Forwarding Adjacencies over MPLS TE Tunnels

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

History for the OSPF Support for Forwarding Adjacencies over MPLS Traffic Engineered Tunnels Feature

Release	Modification
12.0(24)S	This feature was introduced.
12.2(25)S	This feature was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This feature was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
Cisco IOS XE Release 2.1	This feature was implemented on Cisco ASR 1000 series routers.

Finding Feature Information

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

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

Prerequisites for OSPF Forwarding Adjacency

- OSPF must be configured in your network.
- Cisco Express Forwarding (CEF) must be enabled.
- You should understand MPLS TE tunnels for forwarding adjacency as described in the " MPLS Traffic Engineering Forwarding Adjacency" module.

Information About OSPF Forwarding Adjacency

OSPF includes MPLS TE tunnels in the OSPF link-state database in the same way that other links appear for purposes of routing and forwarding traffic. When an MPLS TE tunnel is configured between networking devices, that link is considered a forwarding adjacency. The user can assign a cost to the tunnel to indicate the link's preference. Other networking devices will see the tunnel as a link in addition to the physical link.

How to Configure OSPF Forwarding Adjacency

- Configuring OSPF Forwarding Adjacency, page 238

Configuring OSPF Forwarding Adjacency

Note Configure a forwarding adjacency on two LSP tunnels bidirectionally, from A to B and B to A. Otherwise, the forwarding adjacency is advertised, but not used in the IGP network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **mpls traffic-eng tunnels**
5. **interface loopback** *number*
6. **ip address** *ip-address mask*
7. **no shutdown**
8. **exit**
9. **interface tunnel** *number*
10. **tunnel mode mpls traffic-eng**
11. **tunnel mpls traffic-eng forwarding-adjacency** {**holdtime** *value*}
12. **ip ospf cost** *cost*
13. **exit**
14. **router ospf** *process-id*
15. **mpls traffic-eng router-id** *interface*
16. **mpls traffic-eng area** *number*
17. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip cef distributed** **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding (CEF).

	Command or Action	Purpose
Step 4	**mpls traffic-eng tunnels** **Example:** `Router(config)# mpls traffic-eng tunnels`	Enables MPLS traffic engineering tunnel signaling on a device.
Step 5	**interface loopback** *number* **Example:** `Router(config)# interface loopback0`	Configures a loopback interface and enters interface configuration mode. • Set up a loopback interface with a 32-bit mask, enable CEF, enable MPLS traffic engineering, and set up a routing protocol (OSPF) for the MPLS network.
Step 6	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 10.1.1.1 255.255.255.255`	Configures the IP address and subnet mask of the loopback interface.
Step 7	**no shutdown** **Example:** `Router(config-if)# no shutdown`	Enables the interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 9	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 1`	Designates a tunnel interface for the forwarding adjacency and enters interface configuration mode.
Step 10	**tunnel mode mpls traffic-eng** **Example:** `Router(config-if)# tunnel mode mpls traffic-eng`	Sets the mode of a tunnel to MPLS for traffic engineering.

	Command or Action	Purpose
Step 11	**tunnel mpls traffic-eng forwarding-adjacency** {**holdtime** *value*} **Example:** `Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency holdtime 10000`	Advertises a TE tunnel as a link in an IGP network. • The **holdtime** *value* keyword argument combination is the time in milliseconds (ms) that a TE tunnel waits after going down before informing the network. The range is 0 to 4,294,967,295 ms. The default value is 0.
Step 12	**ip ospf cost** *cost* **Example:** `Router(config-if)# ip ospf cost 4`	(Optional) Configures the cost metric for a tunnel interface to be used as a forwarding adjacency.
Step 13	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 14	**router ospf** *process-id* **Example:** `Router(config)# router ospf 1`	Configures an OSPF routing process and enters router configuration mode.
Step 15	**mpls traffic-eng router-id** *interface* **Example:** `Router(config-router)# mpls traffic-eng router-id ethernet 1/0`	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
Step 16	**mpls traffic-eng area** *number* **Example:** `Router(config-router)# mpls traffic-eng area 1`	Configures a router running OSPF MPLS so that it floods traffic engineering for the indicated OSPF area.
Step 17	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode.

Configuration Examples for OSPF Forwarding Adjacency

Example OSPF Forwarding Adjacency

In the following example, the tunnel destination is the loopback interface on the other router. The router is configured with OSPF TE extensions and it floods traffic engineering link-state advertisements (LSAs) in OSPF area 0. The traffic engineering router identifier for the node is the IP address associated with Loopback 0. The last five lines of the example set up the routing protocol for the MPLS network, which is OSPF in this case.

Note Do not use the **mpls traffic-eng autoroute announce** command if you configure a forwarding adjacency in the tunnel.

```
ip routing
ip cef distributed
mpls traffic-eng tunnels
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
 no shutdown
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.1.1.1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency holdtime 10000
 ip ospf cost 4
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth  10
 tunnel mpls traffic-eng path-option 2 dynamic
router ospf 5
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
 mpls traffic-eng router-id loopback0
 mpls traffic-eng area 0
```

When you look at the self-generated router LSA, you will see it as one of the links in router LSA (shown in bold in the following output).

```
Router# show ip ospf database route self-originate
OSPF Router with ID (10.5.5.5) (Process ID 5)
                Router Link States (Area 0)
  LS age:332
  Options:(No TOS-capability, DC)
  LS Type:Router Links
  Link State ID:10.5.5.5
  Advertising Router:10.5.5.5
  LS Seq Number:80000004
  Checksum:0x1D24
  Length:72
  Number of Links:4
    Link connected to another Router (point-to-point)
     (Link ID) Neighboring Router ID:10.3.3.3
     (Link Data) Router Interface address:0.0.0.23
      Number of TOS metrics:0
       TOS 0 Metrics:1562
    Link connected to:a Transit Network
```

```
 (Link ID) Designated Router address:172.16.0.1
 (Link Data) Router Interface address:172.16.0.2
  Number of TOS metrics:0
   TOS 0 Metrics:10
Link connected to:a Transit Network
 (Link ID) Designated Router address:172.16.0.3
 (Link Data) Router Interface address:172.16.0.4
  Number of TOS metrics:0
   TOS 0 Metrics:10
Link connected to:a Stub Network
 (Link ID) Network/subnet number:10.5.5.5
 (Link Data) Network Mask:255.255.255.255
  Number of TOS metrics:0
   TOS 0 Metrics:1
```

Additional References

The following sections provide references related to OSPF Forwarding Adjacency.

Related Documents

Related Topic	Document Title
MPLS traffic engineering forwarding adjacency	MPLS Traffic Engineering Forwarding Adjacency
Configuring OSPF for MPLS traffic engineering	MPLS Traffic Engineering and Enhancements
MPLS Traffic Engineering - LSP Attributes	MPLS Traffic Engineering - LSP Attributes

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Enabling OSPFv2 on an Interface Basis

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

Finding Feature Information

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

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

Prerequisites for Enabling OSPFv2 on an Interface Basis

OSPFv2 must be running on your network.

Restrictions on Enabling OSPFv2 on an Interface Basis

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

Information About Enabling OSPFv2 on an Interface Basis

Benefits of Enabling OSPFv2 on an Interface Basis

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

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

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

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

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

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

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

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

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

Interface Is Not Configured by network area Command

If the interface is not enabled in OSPFv2 by the **network area** command, the area and OSPF router instance will be created if needed. When the router is reloaded, the OSPF process will not begin running until system initialization is complete. To remove an OSPF router instance, enter the **no router ospf** command. Removing the **ip ospf area** command in interface mode will not result in removing an OSPF router instance.

Removing an ip ospf area Command

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

New Processes

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

Link-State Advertisements and Shortest Path First

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

How to Enable OSPFv2 on an Interface Basis

- Enabling OSPFv2 on an Interface, page 247

Enabling OSPFv2 on an Interface

SUMMARY STEPS

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

DETAILED STEPS

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

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

Configuration Example for Enabling OSPFv2 on an Interface

Example Enabling OSPFv2 on an Interface

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

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# bandwidth 10000
Router(config-if)# ip address 172.16.1.1 255.255.255.0
Router(config-if)# ip ospf hello-interval 1
Router(config-if)# ip ospf 1 area 0
```

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

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

Additional References

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

Related Documents

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

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 2328	*OSPF Version 2*

Technical Assistance

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

Feature Information for Enabling OSPFv2 on an Interface Basis

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

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

Table 27 Feature Information for Enabling OSPFv2 on an Interface Basis

Feature Name	Releases	Feature Information
Enabling OSPFv2 on an Interface Basis **Note** This feature was originally named "Area Command in Interface Mode for OSPFv2."	Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.6	This document describes how to enable OSPFv2 on a per-interface basis to simplify the configuration of unnumbered interfaces. The **ip ospf area** command allows you to enable OSPFv2 explicitly on an interface. The **ip ospf area** command is an alternative to enabling OSPFv2 through the address of the interface that matches the address range specified by the **network area** command. The following commands are introduced or modified in the feature documented in this module: • **ip ospf area.**

OSPF NSR

The OSPF NSR feature allows a router with redundant Route Processors (RPs)to maintain its Open Shortest Path First (OSPF) state and adjacencies across planned and unplanned RP switchovers. It does this by checkpointing state information from OSPF on the active RP to the standby RP. Later, following a switchover to the standby RP, OSPF can use this checkpointed information to continue operation without interruption.

Finding Feature Information

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

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

Prerequisites for OSPF NSR

- OSPF NSR is available for platforms with redundant RPs or Cisco IOS software redundancy running Cisco IOS Release XE 3.3S or later releases.

Restrictions for OSPF NSR

- OSPF nonstop routing (NSR) can significantly increase the memory used by OSPF during certain phases of its operation. CPU usage also can be increased. You should be aware of router memory capacity and estimate the likely memory requirements of OSPF NSR. For more information see

Configuring OSPF NSR. For routers where memory and CPU are constrained you might want to consider using OSPF NSF instead. For more information, see OSPF RFC 3623 Graceful Restart Helper Mode.

- A switchover from the active to the standby RP can take several seconds, depending on the hardware platform, and during this time OSPF is unable to send Hello packets. As a result, configurations that use small OSPF dead intervals might not be able to maintain adjacencies across a switchover.

Information About OSPF NSR

- OSPF NSR Functionality, page 254

OSPF NSR Functionality

Although OSPF NSR serves a similar function to OSPF NSF, it works differently. With NSF, OSPF on the newly active standby RP initially has no state information, so it uses extensions to the OSPF protocol to recover its state from neighboring OSPF routers. For this to work, the neighbors must support the NSF protocol extensions and be willing to act as "helpers" to the restarting router. They must also continue forwarding data traffic to the restarting router while this recovery is taking place.

With NSR, by contrast, the router performing the switchover preserves its state internally, and in most cases the neighbors are unaware that anything has happened. Because no assistance is needed from neighboring routers, NSR can be used in situations where NSF cannot; for example, in networks where not all the neighbors implement the NSF protocol extensions, or where network topology changes during the recovery can make NSF unreliable.

How to Configure OSPF NSR

- Configuring OSPF NSR, page 254

Configuring OSPF NSR

Perform this task to configure OSPF NSR.

NSR adds a single new line, "nsr," to the OSPF router mode configuration. Routers that do not support NSR, for whatever reason, will not accept this command.

Note >

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **n sr**
5. **end**
6. **show ip ospf [** *process-id* **] nsr [[objects]|[statistics]]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 109`	Places the router in router configuration mode and configures an OSPF routing process.
Step 4	**n sr** **Example:** `Router(config-router)# nsr`	Configures NSR.
Step 5	**end** **Example:** `Router(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Command or Action	Purpose
Step 6 **show ip ospf [** *process-id* **] nsr** [**[objects]**|**[statistics]**] **Example:** `Router# show ip ospf 109 nsr`	Displays OSPF NSR status information.

- Troubleshooting Tips, page 256

Troubleshooting Tips

OSPF NSR can increase the amount of memory used by the OSPF router process. To determine how much memory OSPF is currently using without NSR you can use the **show processes** and **show processes memory** commands:

```
Router# show processes
 | include OSPF
 276 Mwe  133BE14         1900       1792    1060 8904/12000  0 OSPF-1 Router
 296 Mwe  133A824           10        971      10 8640/12000  0 OSPF-1 Hello
```

Process 276 is the OSPF router process that is to be checked. The **show processes memory** command is used to display its current memory use:

```
Router# show processes memory 276
Process ID: 276
Process Name: OSPF-1 Router
Total Memory Held: 4454800 bytes
```

In this case OSPF is using 4,454,800 bytes or approximately 4.5 megabytes (MB). OSPF NSR could double this for brief periods, so you should make sure the router has at least 5 MB of free memory before enabling OSPF NSR.

Configuration Examples for OSPF NSR

- Example Configuring OSPF NSR, page 256

Example Configuring OSPF NSR

The following example shows how to configure OSPF NSR:

```
router> enable
Router# configure terminal
Router(config)# router ospf 1
Router(config-router)# nsr
Router(config-router)# end
Router# show ip ospf 1 nsr
Standby RP
 Operating in duplex mode
 Redundancy state: STANDBY HOT
 Peer redundancy state: ACTIVE
 ISSU negotation complete
 ISSU versions compatible
Routing Process "ospf 1" with ID 10.1.1.100
```

```
NSR configured
Checkpoint message sequence number: 3290
Standby synchronization state: synchronized
Bulk sync operations:  1
Last sync start time:  15:22:48.971 UTC Fri Jan 14 2011
Last sync finish time: 15:22:48.971 UTC Fri Jan 14 2011
Last sync lost time:   -
Last sync reset time:  -
LSA Count: 2, Checksum Sum 0x00008AB4
```

The output shows that OSPF NSR is configured and that OSPF on the standby RP is fully synchronized and ready to continue operation should the active RP fail or if a manual switchover is performed.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	*Cisco IOS IP Routing: OSPF Command Reference*
Configuring IETF NSF or Cisco NSF	NSF--OSPF (RFC 3623 OSPF Graceful Restart)

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
RFC 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 NSR

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

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

Table 28 Feature Information for OSPF NSR

Feature Name	Releases	Feature Information
OSPF NSR	XE 3.3S	The OSPF NSR feature allows a router with redundant route processors to maintain its OSPF state and adjacencies across planned and unplanned RP switchovers. In Cisco IOS Release XE 3.3S, this feature was introduced. The following commands were introduced or modified: **nsr, show ip ospf nsr**.

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

OSPFv2 Loop-Free Alternate Fast Reroute

The OSPFv2 Loop-Free Alternate Fast Reroute feature uses a precomputed alternate next hop to reduce failure reaction time when the primary next hop fails. It lets you configure a per-prefix loop-free alternate (LFA) path that redirects traffic to a next hop other than the primary neighbor. The forwarding decision is made and service is restored without other routers' knowledge of the failure.

Finding Feature Information

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

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

Prerequisites for OSPFv2 Loop-Free Alternate Fast Reroute

Open Shortest Path First (OSPF) supports IP FRR only on platforms that support this feature in the forwarding plane. See the Cisco Feature Navigator, http://www.cisco.com/go/cfn , for information on platform support. An account on Cisco.com is not required.

Restrictions for OSPFv2 Loop-Free Alternate Fast Reroute

The OSPFv2 Loop-Free Alternate Fast Reroute feature is not supported on routers that are virtual links headends.

The OSPFv2 Loop-Free Alternate Fast Reroute feature is supported only in global VPN routing and forwarding (VRF) OSPF instances.

You cannot configure a traffic engineering (TE) tunnel interface as a protected interface. Use the MPLS Traffic Engineering--Fast Reroute Link and Node Protection feature to protect these tunnels. See the "MPLS Traffic Engineering--Fast Reroute Link and Node Protection" section in the *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* for more information.

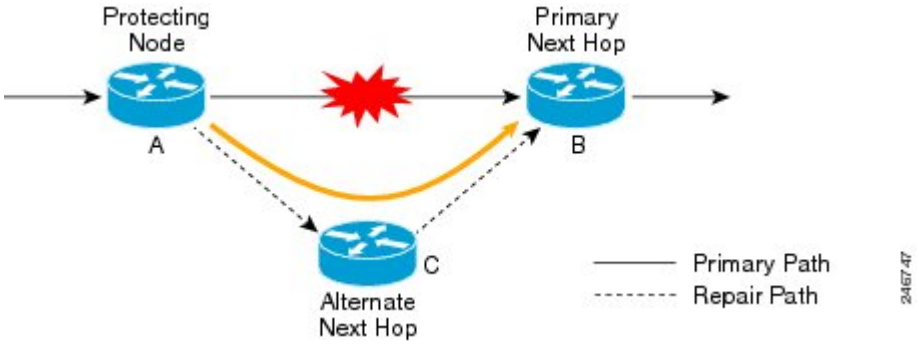
You can configure a TE tunnel interface in a repair path, but OSPF will not verify the tunnel's placement; you must ensure that it is not crossing the physical interface it is intended to protect.

Not all routes can have repair paths. Multipath primary routes might have repair paths for all, some, or no primary paths, depending on network topology, the connectivity of the computing router, and the attributes required of repair paths.

Information About OSPFv2 Loop-Free Alternate Fast Reroute

LFA Repair Paths

The figure below shows how the OSPFv2 Loop-Free Alternate Fast Reroute feature reroutes traffic if a link fails. A protecting router precomputes per-prefix repair paths and installs them in the global Routing Information Base (RIB). When the protected primary path fails, the protecting router diverts live traffic from the primary path to the stored repair path, without other routers' having to recompute network topology or even be aware that the network topology has changed.



LFA Repair Path Attributes

When a primary path fails, many paths are possible repair candidates. The OSPFv2 Loop-Free Alternate Fast Reroute feature default selection policy prioritizes attributes in the following order:

1. srlg
2. primary-path
3. interface-disjoint
4. lowest-metric
5. linecard-disjoint
6. node-protecting
7. broadcast-interface-disjoint

If the evaluation does not select any candidate, the repair path is selected by implicit load balancing. This means that repair path selection varies depending on prefix.

You can use the **show ip ospf fast-reroute** command to display the current configuration.

You can use the **fast-reroute tie-break** command to configure one or more of the repair-path attributes described in the following sections to select among the candidates:

Shared Risk Link Groups

A shared risk link group (SRLG) is a group of next-hop interfaces of repair and protected primary paths that have a high likelihood of failing simultaneously. The OSPFv2 Loop-Free Alternate Fast Reroute feature supports only SRLGs that are locally configured on the computing router. VLANs on a single physical interface are an example of an SRLG. If the physical interface fails, all the VLAN interfaces will fail at the same time. The default repair-path attributes might result in the primary path on one VLAN being protected by a repair path over another VLAN. You can configure the srlg attribute to specify that LFA repair paths do not share the same SRLG ID as the primary path. Use the **srlg** command to assign an interface to an SRLG.

Interface Protection

Point-to-point interfaces have no alternate next hop for rerouting if the primary gateway fails. You can set the interface-disjoint attribute to prevent selection of such repair paths, thus protecting the interface.

Broadcast Interface Protection

LFA repair paths protect links when a repair path and a protected primary path use different next-hop interfaces. However, on broadcast interfaces, if the LFA repair path is computed via the same interface as the primary path, but their next-hop gateways are different, the node is protected but the link might not be. You can set the broadcast-interface-disjoint attribute to specify that the repair path never crosses the broadcast network the primary path points to; that is, it cannot use the interface and the broadcast network connected to it.

See " Broadcast and Non-Broadcast Multi-Access (NBMA) Links " in RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates* for information on network topologies that require this tiebreaker.

Node Protection

The default repair-path attributes might not protect the router that is the next hop in a primary path. You can configure the node-protecting attribute to specify that the repair path will bypass the primary-path gateway router.

Downstream Path

In the case of a high-level network failure or multiple simultaneous network failures, traffic sent over an alternate path might loop until OSPF recomputes the primary paths. You can configure the downstream attribute to specify that the metric of any repair path to the protected destination must be lower than that of the protecting node to the destination. This might result in lost traffic but it prevents looping.

Line-Card Disjoint Interfaces

Line-card interfaces are similar to SRLGs because all interfaces on the same line card will fail at the same time if there is a problem with the line card, for example, line card online insertion and removal (OIR). You can configure the linecard-disjoint attribute to specify that LFA repair paths use different interfaces than those on the primary-path line card.

Metric

An LFA repair path need not be the most efficient of the candidates. A high-cost repair path might be considered more attractive if it provides protection against higher-level network failures. You can configure the metric attribute to specify a repair-path policy that has the lowest metric.

Equal-Cost Multipath Primary Paths

Equal-cost multipath paths (ECMPs) found during the primary shortest path first (SPF) repair, might not be desirable in network designs where traffic is known to exceed the capacity of any single link. You can configure the primary-path attribute to specify an LFA repair path from the ECMP set, or the secondary-path attribute to specify an LFA repair path that is not from the ECMP set.

Candidate Repair-Path Lists

When OSPF computes a repair path, it keeps in the local RIB only the best from among all the candidate paths, in order to conserve memory. You can use the **fast-reroute keep-all-paths** command to create a list of all the candidate repair paths that were considered. This information can be useful for troubleshooting but it can greatly increase memory consumption so it should be reserved for testing and debugging.

How to Configure OSPFv2 Loop-Free Alternate Fast Reroute

Enabling Per-Prefix OSPFv2 Loop-Free Alternate Fast Reroute

Perform this task to enable per-prefix OSPFv2 Loop-Free Alternate Fast Reroute and select the prefix priority in an OSPF area.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix enable prefix-priority** *priority-level*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix enable prefix-priority** *priority-level* **Example:** `Router (config-router)# fast-reroute per-prefix enable prefix-priority low`	Enables repair-path computation and selects the priority level for repair paths. • Low priority specifies that all prefixes have the same eligibility for protection. High priority specifies that only high-priority prefixes are protected.
Step 5	**exit** **Example:** `Router (config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Specifying Prefixes to Be Protected by LFA FRR

Perform this task to specify which prefixes will be protected by LFA FRR. Only prefixes specified in the route map will be protected.

Note Only the following three match keywords are recognized in the route map: **match tag**, **match route-type**, and **match ip address prefix-list**.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **route-map** *map-tag* [permit | deny] [*sequence-number*]
4. **match tag** *tag-name*
5. **exit**
6. **router ospf** *process-id*
7. **prefix-priority** *priority-level* **route-map** *map-tag*
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**route-map** *map-tag* [permit | deny] [*sequence-number*] **Example:** `Router(config)# route-map OSPF-PREFIX-PRIORITY`	Enters route-map configuration mode and specifies the map name.
Step 4	**match tag** *tag-name* **Example:** `Router(config-route-map)# match tag 886`	Specifies the prefixes to be matched. • Only prefixes that match the tag will be protected.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-route-map)# exit`	Exits route-map configuration mode and returns to global configuration mode.
Step 6	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 7	**prefix-priority** *priority-level* **route-map** *map-tag* **Example:** `Router(config-router)# prefix-priority high route-map OSPF-PREFIX-PRIORITY`	Sets the priority level for repair paths and specifies the route map that defines the prefixes.
Step 8	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Configuring a Repair Path Selection Policy

Perform this task to configure a repair path selection policy, specifying a tiebreaking condition. See the LFA Repair Path Attributes, page 262 for information on tiebreaking attributes.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute per-prefix tie-break** *attribute* **[required] index** *index-level*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute per-prefix tie-break** *attribute* **[required] index** *index-level* **Example:** `Router(config-router)# fast-reroute per-prefix tie-break srlg required index 10`	Configures a repair path selection policy by specifying a tiebreaking condition and setting its priority level.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Creating a List of Repair Paths Considered

Perform this task to create a list of paths considered for LFA FRR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **fast-reroute keep-all-paths**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**router ospf** *process-id* **Example:** `Router(config)# router ospf 10`	Enables OSPF routing and enters router configuration mode.
Step 4	**fast-reroute keep-all-paths** **Example:** `Router(config-router)# fast-reroute keep-all-paths`	Specifies creating a list of repair paths considered for LFA FRR.
Step 5	**exit** **Example:** `Router(config-router)# exit`	Exits router configuration mode and returns to global configuration mode.

Prohibiting an Interface From Being Used as the Next Hop

Perform this task to prohibit an interface from being used as the next hop in a repair path.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip ospf fast-reroute per-prefix candidate disable**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet 0/0/0`	Enters interface configuration mode for the interface specified.
Step 4	**ip ospf fast-reroute per-prefix candidate disable** **Example:** `Router(config-if)# ip ospf fast-reroute per-prefix candidate disable`	Prohibits the interface from being used as the next hop in a repair path.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

Configuration Examples for OSPFv2 Loop-Free Alternate Fast Reroute

Example Enabling Per-Prefix LFA IP FRR

The following example shows how to enable per-prefix OSPFv2 Loop-Free Alternate Fast Reroute and select the prefix priority in an OSPF area:

```
Router(config)# router ospf 10
fast-reroute per-prefix enable prefix-priority low
```

Example Specifying Prefix-Protection Priority

The following example shows how to specify which prefixes will be protected by LFA FRR:

```
Router(config)# router ospf 10
prefix-priority high route-map OSPF-PREFIX-PRIORITY
fast-reroute per-prefix enable prefix-priority high
network 192.0.2.1 255.255.255.0 area 0
route-map OSPF-PREFIX-PRIORITY permit 10
match tag 866
```

Example Configuring Repair-Path Selection Policy

The following example shows how to configure a repair-path selection policy that sets SRLG, line card failure and downstream as tiebreaking attributes, and sets their priority indexes:

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute per-prefix tie-break srlg required index 10
  fast-reroute per-prefix tie-break linecard-disjoint index 15
  fast-reroute per-prefix tie-break downstream index 20
  network 192.0.2.1 255.255.255.0 area 0
```

Example Auditing Repair-Path Selection

The following example shows how to keep a record of repair-path selection:

```
router ospf 10
  fast-reroute per-prefix enable prefix-priority low
  fast-reroute keep-all-paths
  network 192.0.2.1 255.255.255.0 area 0
```

Example Prohibiting an Interface from Being a Protecting Interface

The following example shows how to prohibit an interface from being a protecting interface:

```
Router(config)# interface GigabitEthernet 0/0/0
  ip addres
s 192.0.2.1 255.255.255.0
  ip ospf fast-reroute per-prefix candidate disable
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
OSPF commands	Cisco IOS IP Routing: OSPF Command Reference
Protecting TE tunnel interfaces	MPLS Traffic Engineering--Fast Reroute Link and Node Protection section in the *Cisco IOS XE Multiprotocol Label Switching Configuration Guide*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for OSPFv2 Loop-Free Alternate Fast Reroute

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

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

Table 29 Feature Information for OSPFv2 Loop-Free Alternate Fast Reroute

Feature Name	Releases	Feature Information
OSPFv2 Loop-Free Alternate Fast Reroute	Cisco IOS XE Release 3.4S	This feature uses a precomputed alternate next hop to reduce failure reaction time when the primary next hop fails. The following commands were introduced or modified: **debug ip ospf fast-reroute, fast-reroute keep-all-paths, fast-reroute per-prefix (OSPF), fast-reroute tie-break (OSPF), ip ospf fast-reroute per-prefix, prefix-priority, show ip ospf fast-reroute**, **show ip ospf interface**, **show ip ospf neighbor**, **show ip ospf rib .**