THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.

© 2011 Cisco Systems, Inc. All rights reserved.
CONTENTS

Configuring OSPF 1

Finding Feature Information 1

Information About OSPF 1

Cisco OSPF Implementation 2

Router Coordination for OSPF 2

Route Distribution for OSPF 2

  OSPF Network Types 3

  Original LSA Behavior 7

  LSA Group Pacing with Multiple Timers 7

How to Configure OSPF 9

Enabling OSPF 10

Configuring OSPF Interface Parameters 11

Configuring OSPF over Different Physical Networks 11

  Configuring Point-to-Multipoint Broadcast Networks 11

  Configuring OSPF for Nonbroadcast Networks 11

Configuring OSPF Area Parameters 12

Configuring OSPF NSSA 12

  Configuring an OSPF NSSA Area and Its Parameters 12

  Configuring an NSSA ABR as a Forced NSSA LSA Translator 14

  Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility 15

Configuring OSPF NSSA Parameters 16

  Prerequisites 16

Configuring Route Summarization Between OSPF Areas 16

Configuring Route Summarization When Redistributing Routes into OSPF 16

Establishing Virtual Links 17

Generating a Default Route 17

Configuring Lookup of DNS Names 17

Forcing the Router ID Choice with a Loopback Interface 17

Controlling Default Metrics 18
## Contents

- Changing the OSPF Administrative Distances 18
- Configuring OSPF on Simplex Ethernet Interfaces 18
- Configuring Route Calculation Timers 18
- Configuring OSPF over On-Demand Circuits 18
  - Prerequisites 19
- Logging Neighbors Going Up or Down 19
  - Changing the LSA Group Pacing Interval 20
- Blocking OSPF LSA Flooding 20
- Reducing LSA Flooding 20
- Ignoring MOSPF LSA Packets 20
- Displaying OSPF Update Packet Pacing 20
- Monitoring and Maintaining OSPF 21
  - Restrictions 23
- Configuration Examples for OSPF 23
  - Example: OSPF Point-to-Multipoint 24
  - Example: OSPF Point-to-Multipoint with Broadcast 25
  - Example: OSPF Point-to-Multipoint with Nonbroadcast 26
  - Example: Variable-Length Subnet Masks 27
  - Example: OSPF NSSA 27
  - Example: OSPF NSSA Area with RFC 3101 Disabled and RFC 1587 Active 32
  - Example: OSPF Routing and Route Redistribution 33
    - Example: Basic OSPF Configuration 33
    - Example: Basic OSPF Configuration for Internal Router ABR and ASBRs 34
    - Example: Complex Internal Router with ABR and ASBR 35
  - Example: Complex OSPF Configuration for ABR 37
  - Examples: Route Map 38
  - Example: Changing OSPF Administrative Distance 40
  - Example: OSPF over On-Demand Routing 41
  - Example: LSA Group Pacing 42
  - Example: Block LSA Flooding 42
  - Example: Ignore MOSPF LSA Packets 42
- Additional References 42
  - Feature Information for Configuring OSPF 44

### OSPF Stub Router Advertisement 47
  - Finding Feature Information 47
## Contents

- Example Flood Pacing 62
- Example Retransmission Pacing 62
- Example Group Pacing 62
- Additional References 62

### OSPF Sham-Link Support for MPLS VPN 65

- Finding Feature Information 65
- Feature Overview 65
  - Using OSPF in PE-CE Router Connections 66
  - Using a Sham-Link to Correct OSPF Backdoor Routing 66
  - Sham-Link Configuration Example 69
- Benefits 71
- Restrictions 71
- Related Features and Technologies 71
- Related Documents 71
- Supported Platforms 71
- Supported Standards MIBs and RFCs 72
- Prerequisites 73
- Configuration Tasks 73
  - Creating a Sham-Link 73
  - Verifying Sham-Link Creation 75
- Monitoring and Maintaining a Sham-Link 75
- Configuration Examples 75
- Glossary 76

### OSPF Sham-Link MIB Support 79

- Finding Feature Information 79
- Prerequisites for OSPF Sham-Link MIB Support 80
- Restrictions for OSPF Sham-Link MIB Support 80
- Information About OSPF Sham-Link MIB Support 80
  - OSPF Sham-Links in PE-PE Router Connections 80
  - Cisco OSPF MIB and Cisco OSPF Trap MIB Enhancements 80
    - OSPF Sham-Link Configuration Support 80
    - OSPF Sham-Link Neighbor Support 81
    - OSPF Sham-Link Interface Transition State Change Support 81
    - OSPF Sham-Link Neighbor Transition State Change Support 81
Example OSPF Fast Hello Packets 126

Additional References 126

Feature Information for OSPF Support for Fast Hello Packets 127

**OSPF Incremental SPF** 129

Finding Feature Information 129

Prerequisites for OSPF Incremental SPF 129

Information About OSPF Incremental SPF 129

How to Enable OSPF Incremental SPF 130

   Enabling Incremental SPF 130

Configuration Examples for OSPF Incremental SPF 131

   Example Incremental SPF 131

Additional References 131

Feature Information for OSPF Incremental SPF 132

**OSPF Limit on Number of Redistributed Routes** 135

Finding Feature Information 135

Prerequisites for OSPF Limit on Number of Redistributed Routes 135

Information About OSPF Limit on Number of Redistributed Routes 135

How to Configure OSPF Limit the Number of OSPF Redistributed Routes 136

   Limiting the Number of OSPF Redistributed Routes 136

   Requesting a Warning About the Number of Routes Redistributed into OSPF 138

Configuration Examples for OSPF Limit on Number of Redistributed Routes 139

   Example OSPF Limit on Number of Redistributed Routes 139

   Example Requesting a Warning About the Number of Redistributed Routes 140

Additional References 140

Feature Information for OSPF Limit on Number of Redistributed Routes 141

**OSPF Link-State Advertisement Throttling** 143

Finding Feature Information 143

Prerequisites for OSPF LSA Throttling 144

Information About OSPF LSA Throttling 144

   Benefits of OSPF LSA Throttling 144

   How OSPF LSA Throttling Works 144

How to Customize OSPF LSA Throttling 144

   Customizing OSPF LSA Throttling 145

Configuration Examples for OSPF LSA Throttling 150

   Example OSPF LSA Throttling 150
Configuring OSPF

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

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

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

- Finding Feature Information, page 1
- Information About OSPF, page 1
- How to Configure OSPF, page 9
- Configuration Examples for OSPF, page 23
- Additional References, page 42
- Feature Information for Configuring OSPF, page 44

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, page 2
- Router Coordination for OSPF, page 2
- Route Distribution for OSPF, page 2
Cisco OSPF Implementation

The Cisco implementation conforms to the OSPF Version 2 specifications detailed in the Internet RFC 2328. The list that follows 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.
- OSPF over demand circuit--RFC 1793.

Router Coordination for OSPF

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

Route Distribution for OSPF

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

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

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

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

You can configure your network as either a broadcast or an NBMA network.
X.25 and Frame Relay provide an optional broadcast capability that can be configured in the map to allow OSPF to run as a broadcast network. Refer to the x25 map and frame-relay map command descriptions in the Cisco IOS Wide-Area Networking Command Reference publication for more detail.

- OSPF Network Types, page 3
- Original LSA Behavior, page 7
- LSA Group Pacing with Multiple Timers, page 7

### OSPF Network Types

You have the choice of configuring your OSPF network type as either broadcast or NBMA, regardless of the default media type. Using this feature, you can configure broadcast networks as NBMA networks when, for example, you have routers in your network that do not support multicast addressing. You also can configure NBMA networks (such as X.25, Frame Relay, and SMDS) as broadcast networks. This feature saves you from needing to configure neighbors, as described in the section "Configuring OSPF for Nonbroadcast Networks, page 11" 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.

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

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

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

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

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

You can specify the following neighbor parameters, as required:
On point-to-multipoint, nonbroadcast networks, use the **neighbor** router configuration command to identify neighbors. Assigning a cost to a neighbor is optional.

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

On any point-to-multipoint interface (broadcast or not), the Cisco IOS 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 15.1(2)S 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 Release 11.2. 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 15.1(2)S 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.
Even a forced translator might not translate all LSAs; translation depends on the contents of each LSA.

The figure below shows a network diagram in which OSPF Area 1 is defined as the stub area. The Enhanced Interior Gateway Routing Protocol (EIGRP) routes cannot be propagated into the OSPF domain because routing redistribution is not allowed in the stub area. However, once OSPF Area 1 is defined as an NSSA, an NSSA ASBR can inject the EIGRP routes into the OSPF NSSA by creating Type 7 LSAs.

Figure 1    OSPF NSSA

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

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

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

In OSPF, all areas must be connected to a backbone area. If there is a break in backbone continuity, or the backbone is purposefully partitioned, you can establish a virtual link. The two endpoints of a virtual link are ABRs. The virtual link must be configured in both routers. The configuration information in each router consists of the other virtual endpoint (the other ABR) and the nonbackbone area that the two routers have in common (called the transit area). Note that virtual links cannot be configured through stub areas.

You can force an ASBR to generate a default route into an OSPF routing domain. Whenever you specifically configure redistribution of routes into an OSPF routing domain, the router automatically
becomes an ASBR. However, an ASBR does not, by default, generate a 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 software will use this IP address as its router ID, even if other interfaces have larger IP addresses. Because loopback interfaces never go down, greater stability in the routing table is achieved.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Original LSA Behavior**

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

All LSAs refreshed, 120 external LSAs on Ethernet need three packets

Prior to pacing, all LSAs refreshed at once

**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

Without group pacing, LSAs need to be refreshed frequently and at random intervals. Individual LSA timers require many refresh packets that contain few LSAs. 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 in IGPs such as OSPF. By design, OSPF requires LSAs to be refreshed as they expire after 3600 seconds. Some implementations have tried to improve the flooding by reducing the frequency to refresh from 30 minutes to about 50 minutes. This solution reduces the amount of refresh traffic but requires at least one refresh before the LSA expires. The OSPF flooding reduction solution works by reducing unnecessary refreshing and flooding of already known and unchanged information. To achieve this reduction, the LSAs are now flooded with the higher bit set. The LSAs are now set as "do not age."

Cisco routers do not support LSA Type 6 Multicast OSPF (MOSPF), and they generate syslog messages if they receive such packets. If the router is receiving many MOSPF packets, you might want to configure the router to ignore the packets and thus prevent a large number of syslog messages.
The former OSPF implementation for sending update packets needed to be more efficient. Some update packets were getting lost in cases where the link was slow, a neighbor could not receive the updates quickly enough, or the router was out of buffer space. For example, packets might be dropped if either of the following topologies existed:

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

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

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

How to Configure OSPF

To configure OSPF, perform the tasks described in the following sections. The tasks in the Enabling OSPF section are required; the tasks in the remaining sections are optional, but might be required for your application. For information about the maximum number of interfaces, see the Restrictions, page 23.

- Enabling OSPF, page 10
- Configuring OSPF Interface Parameters, page 11
- Configuring OSPF over Different Physical Networks, page 11
- Configuring OSPF Area Parameters, page 12
- Configuring OSPF NSSA, page 12
- Configuring OSPF NSSA Parameters, page 16
- Configuring Route Summarization Between OSPF Areas, page 16
- Configuring Route Summarization When Redistributing Routes into OSPF, page 16
- Establishing Virtual Links, page 17
- Generating a Default Route, page 17
- Configuring Lookup of DNS Names, page 17
- Forcing the Router ID Choice with a Loopback Interface, page 17
- Controlling Default Metrics, page 18
- Changing the OSPF Administrative Distances, page 18
- Configuring OSPF on Simplex Ethernet Interfaces, page 18
- Configuring Route Calculation Timers, page 18
- Configuring OSPF over On-Demand Circuits, page 18
- Logging Neighbors Going Up or Down, page 19
- Blocking OSPF LSA Flooding, page 20
- Reducing LSA Flooding, page 20
- Ignoring MOSPF LSA Packets, page 20
- Displaying OSPF Update Packet Pacing, page 20
- Monitoring and Maintaining OSPF, page 21
- Restrictions, page 23
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
| Example:          | - Enter your password if prompted.  
| Router> enable    |         |
| Step 2 configure terminal | Enters global configuration mode.  
| Example:          |         |
| Router# configure terminal |         |
| Step 3 router ospf process-id | Enables OSPF routing, which places the router in router configuration mode.  
| Example:          |         |
| Router(config)# router ospf 109 |         |
| Step 4 network ip-address wildcard-mask area area-id | Defines an interface on which OSPF runs and defines the area ID for that interface.  
| Example:          |         |
| Router(config-router)# network 192.168.129.16 0.0.0.3 area 20 |         |
| Step 5 end        | Exits router configuration mode and returns to privileged EXEC mode.  
| Example:          |         |
| Router(config-router)# end |         |
Configuring OSPF Interface Parameters

Configuring OSPF over Different Physical Networks

- Configuring Point-to-Multipoint Broadcast Networks, page 11
- Configuring OSPF for Nonbroadcast Networks, page 11

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 <code>ip ospf network point-to-multipoint</code></td>
<td>Configures an interface as point-to-multipoint for broadcast media.</td>
</tr>
<tr>
<td>Step 2 <code>exit</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 <code>router ospf process-id</code></td>
<td>Configures an OSPF routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Step 4 <code>neighbor ip-address cost number</code></td>
<td>Specifies a neighbor and assigns a cost to the neighbor.</td>
</tr>
</tbody>
</table>

**Note**  Repeat this step for each neighbor if you want to specify a cost. Otherwise, neighbors will assume the cost of the interface, based on the `ip ospf cost` interface configuration command.

Configuring OSPF for Nonbroadcast Networks

SUMMARY STEPS

1. `ip ospf network point-to-multipoint non-broadcast`
2. `exit`
3. `router ospf process-id`
4. `neighbor ip-address [cost number]`
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> ip ospf network point-to-multipoint non-broadcast</td>
<td>Configures an interface as point-to-multipoint for nonbroadcast media.</td>
</tr>
<tr>
<td><strong>Step 2</strong> exit</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> router ospf process-id</td>
<td>Configures an OSPF routing process and enters router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> neighbor ip-address [cost number]</td>
<td>Specifies a neighbor and assigns a cost to the neighbor. <strong>Note</strong> 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 <code>ip ospf cost</code> interface configuration command.</td>
</tr>
</tbody>
</table>

---

### Configuring OSPF Area Parameters

#### Configuring OSPF NSSA

- Configuring an OSPF NSSA Area and Its Parameters, page 12
- 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 OSPF NSSA Area and Its Parameters

**SUMMARY STEPS**

1. enable
2. configure terminal
3. router ospf process-id
4. redistribute protocol [process-id] [level-1 | level-1-2 | level-2] [autonomous-system-number] [metric [metric-value | transparent]] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets] [nssa-only]
5. network ip-address wildcard-mask area area-id
6. area area-id nssa [no-redistribution] [default-information-originate [metric] [metric-type]] [no-summary] [nssa-only]
7. end
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| Example: | Router# configure terminal |
| **Step 3** router ospf process-id | Enables OSPF routing and enters router configuration mode.  
- The process-id argument identifies the OSPF process. In this example the number of the routing process is 10. |
| Example: | Router(config)# router ospf 10 |
| **Step 4** redistribute protocol [process-id] [level-1 | level-1-2 | level-2] [autonomous-system-number] [metric [metric-value] [transparent]] [metric-type type-value] [match [internal | external 1 | external 2]] [tag tag-value] [route-map map-tag] [subnets] [nssa-only] | Redistributes routes from one routing domain into another routing domain.  
- The example causes RIP subnets to be redistributed into the OSPF domain. |
| Example: | Router(config-router)# redistribute rip subnets |
| **Step 5** network ip-address wildcard-mask area area-id | Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.  
- The example defines 172.19.92.0/0.0.0.255 interfaces for OSPF area 1 for OSPF routing process 10. |
| Example: | Router(config-router)# network 172.19.92.0 0.0.0.255 area 1 |
| **Step 6** area area-id nssa [no-redistribution] [default-information originate] [metric] [metric-type] [no-summary] [nssa-only] | Configures an NSSA area.  
- In the example, area 1 is configured as an NSSA area. |
| Example: | Router(config-router)# area 1 nssa |
Command or Action | Purpose
---|---
Step 7 end | Exits router configuration mode and returns to privileged EXEC mode.

Example:

```
Router(config-router)# end
```

---

### Configuring an NSSA ABR as a Forced NSSA LSA Translator

**Note**

In Cisco IOS Release 15.1(2)S 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
</tbody>
</table>
| ```
Router> enable
``` | • Enter your password if prompted. |
| **Step 2 configure terminal** | Enters global configuration mode. |
| **Example:** | |
| ```
Router# configure terminal
``` | |
| **Step 3 router ospf process-id** | Enables OSPF routing and enters router configuration mode. |
| **Example:** | |
| ```
Router(config)# router ospf 1
``` | • The `process-id` argument identifies the OSPF process. |
### Command or Action | Purpose
--- | ---
**Step 4** area area-id nssa translate type7 always | Configures an NSSA ABR router as a forced NSSA LSA translator. **Note** In Cisco IOS Release 15.1(2)S 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.

Example: 
Router(config-router)# area 10 nssa translate type7 always

**Step 5** end | Exits router configuration mode and returns to privileged EXEC mode.

Example: 
Router(config-router)# end

### Disabling RFC 3101 Compatibility and Enabling RFC 1587 Compatibility

**Note** In Cisco IOS Release 15.1(2)S 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 | Enables privileged EXEC mode.  
• Enter your password if prompted.  

Example:  
Router> enable

**Step 2** configure terminal | Enters global configuration mode.  

Example:  
Router# configure terminal
### Configuring OSPF NSSA Parameters

- **Prerequisites**, page 16

#### Prerequisites

Evaluate the following considerations before you implement this feature:

- You can set a Type 7 default route that can be used to reach external destinations. When configured, the 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.

### Configuring Route Summarization Between OSPF Areas

### Configuring Route Summarization When Redistributing Routes into OSPF

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong> router ospf process-id</td>
<td>Enables OSPF routing and enters router configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** 
  Router(config)# router ospf 1 | - The `process-id` argument identifies the OSPF process. |

| **Step 4** compatible rfc1587 | Changes the method used to perform route selection to RFC 1587 compatibility and disables RFC 3101. |
| **Example:** 
  Router(config-router)# compatible rfc1587 | |

| **Step 5** end | Exits router configuration mode and returns to privileged EXEC mode. |
| **Example:** 
  Router(config-router)# end | |

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary-address {ip-address mask</td>
<td>Specifies an address and mask that covers redistributed routes, so only one summary route is advertised. Use the optional <strong>not-advertise</strong> keyword to filter out a set of routes.</td>
</tr>
<tr>
<td></td>
<td>prefix mask}</td>
</tr>
<tr>
<td></td>
<td>[not-advertise] [tag tag]</td>
</tr>
</tbody>
</table>
Establishing Virtual Links

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>area area-id virtual-link router-id (authentication [message-digest</td>
<td>null]) (hello-interval seconds) (retransmit-interval seconds) (transmit-delay seconds) (dead-interval seconds) (authentication-key key</td>
</tr>
</tbody>
</table>

Generating a Default Route

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-information originate {always} [metric metric-value] [metric-type type-value] [route-map map-name]</td>
<td>Forces the ASBR to generate a default route into the OSPF routing domain. Note: The always keyword includes the following exception when the route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.</td>
</tr>
</tbody>
</table>

Configuring Lookup of DNS Names

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf name-lookup</td>
<td>Configures DNS name lookup.</td>
</tr>
</tbody>
</table>

Forcing the Router ID Choice with a Loopback Interface

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 interface loopback 0</td>
<td>Creates a loopback interface, which places the router in interface configuration mode.</td>
</tr>
<tr>
<td>Step 2 ip address ip-address mask</td>
<td>Assigns an IP address to this interface.</td>
</tr>
</tbody>
</table>
Controlling Default Metrics

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-cost reference-bandwidth ref-bw</td>
<td>Differentiates high-bandwidth links.</td>
</tr>
</tbody>
</table>

Changing the OSPF Administrative Distances

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>distance ospf intra-area</td>
<td>inter-area</td>
</tr>
</tbody>
</table>

Configuring OSPF on Simplex Ethernet Interfaces

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive-interface interface-type interface-number</td>
<td>Suppresses the sending of hello packets through the specified interface.</td>
</tr>
</tbody>
</table>

Configuring Route Calculation Timers

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>timers spf spf-delay spf-holdtime</td>
<td>Configures route calculation timers.</td>
</tr>
</tbody>
</table>

Configuring OSPF over On-Demand Circuits

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>router ospf process-id</code></td>
<td>Enables OSPF operation.</td>
</tr>
<tr>
<td>2</td>
<td><code>interface type number</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>3</td>
<td><code>ip ospf demand-circuit</code></td>
<td>Configures OSPF over an on-demand circuit.</td>
</tr>
</tbody>
</table>
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 the On-Demand Circuits feature:

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

Logging Neighbors Going Up or Down

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>log-adjacency-changes</code></td>
<td>Sends syslog message when an OSPF neighbor goes up or down.</td>
</tr>
<tr>
<td><code>{detail}</code></td>
<td></td>
</tr>
</tbody>
</table>

**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, page 20
### Changing the LSA Group Pacing Interval

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>timers pacing lsa-group <em>seconds</em></td>
<td>Changes the group pacing of LSAs.</td>
</tr>
</tbody>
</table>

### Blocking OSPF LSA Flooding

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf database-filter all out</td>
<td>Blocks the flooding of OSPF LSA packets to the interface.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor <em>ip-address</em> database-filter all out</td>
<td>Blocks the flooding of OSPF LSA packets to the specified neighbor.</td>
</tr>
</tbody>
</table>

### Reducing LSA Flooding

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf flood-reduction</td>
<td>Suppresses the unnecessary flooding of LSAs in stable topologies.</td>
</tr>
</tbody>
</table>

### Ignoring MOSPF LSA Packets

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ignore lsa mospf</td>
<td>Prevents the router from generating syslog messages when it receives MOSPF LSA packets.</td>
</tr>
</tbody>
</table>

### Displaying OSPF Update Packet Pacing

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf flood-list <em>interface-type</em> <em>interface-number</em></td>
<td>Displays a list of LSAs waiting to be flooded over an interface.</td>
</tr>
</tbody>
</table>
## Monitoring and Maintaining OSPF

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip ospf {process-id}</code></td>
<td>Displays general information about OSPF routing processes.</td>
</tr>
<tr>
<td><code>show ip ospf border-routers</code></td>
<td>Displays the internal OSPF routing table entries to the ABR and ASBR.</td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database</code></td>
<td>Displays lists of information related to the OSPF database.</td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {database-summary}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {router} {self-originate}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {router} {adv-router {ip-address}}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {router} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {network} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {summary} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {asbr-summary} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {external} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {nssa-external} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {opaque-link} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {opaque-area} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td><code>show ip ospf {process-id} {area-id} database {opaque-as} {link-state-id}</code></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>show ip ospf flood-list interface type</td>
<td>Displays a list of LSAs waiting to be flooded over an interface (to observe OSPF packet pacing).</td>
</tr>
<tr>
<td>show ip ospf interface {type number}</td>
<td>Displays OSPF-related interface information.</td>
</tr>
<tr>
<td>show ip ospf neighbor {interface-name} {neighbor-id} detail</td>
<td>Displays OSPF neighbor information on a per-interface basis.</td>
</tr>
<tr>
<td>show ip ospf request-list {neighbor} {interface} {interface-neighbor}</td>
<td>Displays a list of all LSAs requested by a router.</td>
</tr>
<tr>
<td>show ip ospf retransmission-list {neighbor} {interface} {interface-neighbor}</td>
<td>Displays a list of all LSAs waiting to be re-sent.</td>
</tr>
<tr>
<td>show ip ospf {process-id} summary-address</td>
<td>Displays a list of all summary address redistribution information configured under an OSPF process.</td>
</tr>
<tr>
<td>show ip ospf virtual-links</td>
<td>Displays OSPF-related virtual links information.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip ospf {pid} {process</td>
<td>redistribution</td>
</tr>
</tbody>
</table>

**Restrictions**

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

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

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

**Configuration Examples for OSPF**
Example: OSPF Point-to-Multipoint

In the figure below, 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
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
!
routing ospf 1
network 10.0.0.0 0.0.0.255 area 0

Router 2 Configuration

hostname Router 2
Example: OSPF Point-to-Multipoint with Broadcast

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

interface Serial0
ip address 10.0.1.1 255.255.255.0
encapsulation frame-relay
ip ospf cost 100
ip ospf network point-to-multipoint
frame-relay map ip 10.0.1.3 202 broadcast
frame-relay map ip 10.0.1.4 203 broadcast
frame-relay map ip 10.0.1.5 204 broadcast
frame-relay local-dlci 200

! router ospf 1
network 10.0.1.0 0.0.0.255 area 0
neighbor 10.0.1.5 cost 5
neighbor 10.0.1.4 cost 10

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

interface serial 0
ip address 10.0.1.3 255.255.255.0
ip ospf network point-to-multipoint
encapsulation frame-relay
frame-relay local-dlci 301
frame-relay map ip 10.0.1.1 300 broadcast
no shutdown

! router ospf 1
 network 10.0.1.0 0.0.0.255 area 0

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

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

The route information in the first configuration is as follows:

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

### Example: OSPF Point-to-Multipoint with Nonbroadcast

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

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

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

```
interface Serial9/2
 ip address 10.0.1.3 255.255.255.0
 encapsulation frame-relay
 ip ospf network point-to-multipoint non-broadcast
 no ip mroute-cache
 no keepalive
 no fair-queue
 frame-relay local-dlci 301
 frame-relay map ip 10.0.1.1 300
 no shutdown
 !
 router ospf 1
 network 10.0.1.0 0.0.0.255 area 0
```

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

```
Router# show ip ospf neighbor
```
Example: Variable-Length Subnet Masks

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

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

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

Example: 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 Ethernet0/0
   ip address 192.168.0.1 255.255.255.0
   ip ospf 1 area 0
   no cdp enable
!
interface Serial10/0
   description Router2 interface s11/0
   ip address 192.168.10.1 255.255.255.0
   ip ospf 1 area 1
   serial restart-delay 0
   no cdp enable
!
router ospf 1
   area 1 nssa
!
end
```

**Router 2**

```
hostname Router2
!
!
interface Loopback1
   ip address 10.1.0.2 255.255.255.255
```
Configuration Examples for OSPF

interface Serial10/0
description Router1 interface s11/0
no ip address
shutdown
serial restart-delay 0
no cdp enable
interface Serial11/0
description Router1 interface s10/0
ip address 192.168.10.2 255.255.255.0
ip ospf 1 area 1
serial restart-delay 0
no cdp enable
interface Serial14/0
description Router3 interface s13/0
ip address 192.168.14.2 255.255.255.0
ip ospf 1 area 1
serial restart-delay 0
no cdp enable
router ospf 1
area 1 nssa
end

Router 3

hostname Router3
!
interface Loopback1
  ip address 10.1.0.3 255.255.255.255
!
interface Ethernet3/0
  ip address 192.168.3.3 255.255.255.0
  no cdp enable
!
interface Serial13/0
description Router2 interface s14/0
ip address 192.168.14.3 255.255.255.0
ip ospf 1 area 1
serial restart-delay 0
no cdp enable
!
router ospf 1
  log-adjacency-changes
  area 1 nssa
  redistribute rip subnets
!
router rip
  version 2
  redistribute ospf 1 metric 15
  network 192.168.3.0
end

Router 4

hostname Router4
!
interface Loopback1
  ip address 10.1.0.4 255.255.255.255
!
interface Ethernet3/0
  ip address 192.168.3.4 255.255.255.0
  no cdp enable
!
interface Ethernet4/1
  ip address 192.168.41.4 255.255.255.0

router rip
version 2
network 192.168.3.0
network 192.168.41.0
!
end

Router 5

hostname Router5
!
interface Loopback1
   ip address 10.1.0.5 255.255.255.255
!
interface Ethernet0/0
   ip address 192.168.0.10 255.255.255.0
   ip ospf 1 area 0
   no cdp enable
!
interface Ethernet1/1
   ip address 192.168.11.10 255.255.255.0
   ip ospf 1 area 0
!
router ospf 1
!
end

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 OSPF 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 SPF s 10000 msecs
- Maximum wait time between two consecutive SPF s 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 0x0000000
- Number of opaque AS LSA 0. Checksum Sum 0x0000000
- 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
  - 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)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.1</td>
<td>10.1.0.1</td>
<td>1990</td>
<td>0x80000016</td>
<td>0x00C0B2</td>
<td>2</td>
</tr>
<tr>
<td>10.1.0.2</td>
<td>10.1.0.2</td>
<td>1753</td>
<td>0x80000016</td>
<td>0x009371</td>
<td>4</td>
</tr>
<tr>
<td>10.1.0.3</td>
<td>10.1.0.3</td>
<td>1903</td>
<td>0x80000016</td>
<td>0x004149</td>
<td>2</td>
</tr>
</tbody>
</table>

Summary Net Link States (Area 1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0</td>
<td>10.1.0.1</td>
<td>1990</td>
<td>0x80000017</td>
<td>0x00A605</td>
</tr>
<tr>
<td>192.168.11.0</td>
<td>10.1.0.1</td>
<td>1990</td>
<td>0x80000015</td>
<td>0x009503</td>
</tr>
</tbody>
</table>

Type-7 AS External Link States (Area 1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.3.0</td>
<td>10.1.0.3</td>
<td>1903</td>
<td>0x80000015</td>
<td>0x00480F</td>
</tr>
<tr>
<td>192.168.41.0</td>
<td>10.1.0.3</td>
<td>1903</td>
<td>0x80000015</td>
<td>0x00A4C0</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>LSA Type</th>
<th>Count</th>
<th>Delete</th>
<th>Maxage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Network</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Summary Net</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Summary ASBR</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Type-7 Ext</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Prefixes redistributed in Type-7 0
| Opaque Link | 0     | 0      | 0      |
| Opaque Area | 0     | 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 SPF requests 10000 msecs
    Maximum wait time between two consecutive SPF requests 10000 msecs
    Incremental-SPF disabled
    Minimum LSA interval 5 secs
    Minimum LSA arrival 1000 msecs
    LSA group pacing timer 240 secs
```
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
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 0x00000000
Number of opaque AS LSA 0. Checksum Sum 0x00000000
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 0x00000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```
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.

Example: OSPF Routing and Route Redistribution

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

Three types of examples follow:

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

  - Example: Basic OSPF Configuration, page 33
  - Example: Basic OSPF Configuration for Internal Router ABR and ASBRs, page 34
  - Example: Complex Internal Router with ABR and ASBR, page 35
  - Example: Complex OSPF Configuration for ABR, page 37

Example: Basic OSPF Configuration

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

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

Example: Basic OSPF Configuration for Internal Router ABR and ASBRs

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

```
router ospf 109
  network 192.168.10.0 0.0.0.255 area 10.9.50.0
  network 192.168.20.0 0.0.255.255 area 2
  network 192.168.30.0 0.0.0.255 area 3
  network 192.168.40.0 255.255.255.255 area 0
!
! Interface Ethernet0 is in area 10.9.50.0:
! interface ethernet 0
  ip address 192.168.10.5 255.255.255.0
!
! Interface Ethernet1 is in area 2:
! interface ethernet 1
  ip address 192.168.20.5 255.255.255.0
!
! Interface Ethernet2 is in area 2:
! interface ethernet 2
  ip address 192.168.20.7 255.255.255.0
!
! Interface Ethernet3 is in area 3:
! interface ethernet 3
  ip address 192.169.30.5 255.255.255.0
!
! Interface Ethernet4 is in area 0:
! interface ethernet 4
  ip address 192.168.40.1 255.255.255.0
!
! Interface Ethernet5 is in area 0:
! interface ethernet 5
  ip address 192.168.40.12 255.255.0.0
```

Each `network area` router configuration command is evaluated sequentially, so the order of these commands in the configuration is important. The Cisco IOS 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 Ethernet interface 0. Ethernet interface 0 is attached to area 10.9.50.0 only.

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

This process of attaching interfaces to OSPF areas continues for all `network area` commands. Note that the last `network area` command in this example is a special case. With this command, all available interfaces (not explicitly attached to another area) are attached to area 0.
Example: Complex Internal Router with ABR and ASBR

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

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

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

**Router B Configuration--Internal Router**

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

**Router C Configuration--ABR**

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

**Router D Configuration--Internal Router**

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

**Router E Configuration--ASBR**

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

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

Configuration tasks associated with redistribution are as follows:

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

The following is an example OSPF configuration:

```bash
interface ethernet 0
  ip address 192.42.110.201 255.255.255.0
  ip ospf authentication-key abcdefgh
  ip ospf cost 10
```
interface ethernet 1
  ip address 172.19.251.202 255.255.255.0
  ip ospf authentication-key ijklmnop
  ip ospf cost 20
  ip ospf retransmit-interval 10
  ip ospf transmit-delay 2
  ip ospf priority 4

interface ethernet 2
  ip address 172.19.254.2 255.255.255.0
  ip ospf authentication-key abcdedefgh
  ip ospf cost 10

interface ethernet 3
  ip address 10.56.0.0 255.255.0.0
  ip ospf authentication-key ijklmnop
  ip ospf cost 20
  ip ospf dead-interval 80

In the following configuration OSPF is on network 172.16.0.0:

router ospf 201
  network 10.10.0.0 0.255.255.255 area 10.10.0.0
  network 192.42.110.0 0.0.0.255 area 192.42.110.0
  network 172.16.0.0 0.0.255.255 area 0
  area 0 authentication
  area 10.10.0.0 stub
  area 10.10.0.0 authentication
  area 10.10.0.0 default-cost 20
  area 192.42.110.0 authentication
  area 10.10.0.0 range 10.10.0.0 255.0.0.0
  area 192.42.110.0 range 192.42.110.0 255.255.255.0
  area 0 range 172.16.251.0 255.255.255.0
  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:

```
routing 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:

```
routing 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.

```
routing 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.

```
routing 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 160.89.0.0 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:

```
routing 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 140.222.0.0 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*
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](image)

Router A Configuration

```plaintext
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

```plaintext
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](image)

Router A Configuration

```plaintext
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
dialer-list 1 protocol ip permit
```
Router B Configuration

username RouterA password 7 04511E0804
isdn switch-type basic-5ess
ip routing
interface Ethernet0
  ip address 192.168.50.16 255.255.255.0
  no shutdown
interface BRI0
  no cdp enable
description connected PBX 1484
  ip address  192.168.45.17 255.255.255.0
  encapsulation ppp
dialer map ip 192.168.45.19 name RouterA broadcast 61485
dialer-group 1
  ppp authentication chap
  no shutdown
  router ospf 100
  network 192.168.45.0 0.0.0.255 area 0
  network 192.168.45.50 0.0.0.255 area 0
  !
dialer-list 1 protocol ip permit

Example: LSA Group Pacing

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

```conf
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 Ethernet interface 0:

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

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

```conf
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:

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

Additional References
### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
<tr>
<td>Protocol-independent features that work with OSPF</td>
<td>&quot;Configuring IP Routing Protocol-Independent Features&quot;</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported, and support for existing standards has not been modified.</td>
</tr>
<tr>
<td></td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified MIBs are supported, and support for existing MIBs has not been modified.</td>
</tr>
<tr>
<td></td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1587</td>
<td>The OSPF NSSA Option, March 1994</td>
</tr>
<tr>
<td>RFC 1793</td>
<td>Extending OSPF to Support Demand Circuits, April 1995</td>
</tr>
<tr>
<td>RFC 2328</td>
<td>OSPF Version 2, April 1998</td>
</tr>
<tr>
<td>RFC 3101</td>
<td>The OSPF NSSA Option, January 2003</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Configuring OSPF

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>11.2.1</td>
<td>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.</td>
</tr>
<tr>
<td>OSPF Flooding Reduction</td>
<td>12.1(2)T</td>
<td>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:</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OSPF Not-So-Stubby Areas</td>
<td>11.2.1</td>
<td>OSPF NSSA is a nonproprietary extension of the existing OSPF stub area feature. This feature is documented in the following sections:</td>
</tr>
<tr>
<td>OSPF Packet Pacing</td>
<td>12.0(1)T</td>
<td>OSPF update packets are automatically paced so they are not sent less than 33 milliseconds apart. This feature is documented in the following section:</td>
</tr>
<tr>
<td>OSPF Support for NSSA RFC 3101</td>
<td>15.1(2)S</td>
<td>This feature adds support for the OSPF NSSA specification described by RFC 3101. RFC3101 replaced RFC 1587 and is backward compatible with RFC1587. The following commands were introduced or modified: area nssa translate. compatible rfc1587.</td>
</tr>
<tr>
<td></td>
<td>15.0(1)SY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.2(2)T</td>
<td></td>
</tr>
<tr>
<td>OSPF - Demand Circuit Disable</td>
<td>15.0(1)SY</td>
<td>The <code>ignore</code> keyword was added to the <code>ip ospf demand-circuit</code> command, allowing you to prevent an interface from accepting demand-circuit requests from other routers.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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, page 47
- Information About OSPF Stub Router Advertisement, page 47
- Supported Platforms, page 49
- How to Configure OSPF Stub Router Advertisement, page 50
- Configuration Examples of OSPF Stub Router Advertisement, page 54
- Additional References, page 54
- Feature Information for OSPF Stub Router Advertisement, page 55

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, page 47
- Allowing Routing Tables to Converge, page 48
- Configuring a Graceful Shutdown, page 48
- Benefits of OSPF Stub Router Advertisement, page 49
- Related Features and Technologies, page 49

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.

---

**Allowing 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.

**Configuring a Graceful Shutdown**

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.
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.

**Related Features and Technologies**

The OSPF Stub Router Advertisement feature is an extension of the OSPF routing protocol. For more information about configuring OSPF and BGP, refer to the *Cisco IOS IP Routing Configuration Guide* and the *Cisco IOS IP Routing Command Reference*.

**Supported Platforms**

The OSPF Stub Router Advertisement feature is supported by the following platforms in Cisco IOS Release 12.2(14)S that support OSPF:

- Cisco 7200 series
- Cisco 7400 series
- Cisco 7500 series

**Determining Platform Support Through Cisco Feature Navigator**

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn
Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

How to Configure OSPF Stub Router Advertisement

See the following sections for configuration tasks to 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 50
- Configuring Advertisement Until Routing Tables Converge, page 50
- Configuring Advertisement for a Graceful Shutdown, page 51
- 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Places the router in router configuration mode and enables an OSPF routing process.</td>
</tr>
<tr>
<td>Step 2</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

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

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)# exit
4. Router(config)# exit
5. Router# show ip ospf

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router(config)# router ospf process-id</td>
<td>Places the router in router configuration mode and enables an OSPF routing process.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Router(config-router)# max-metric router-lsa</td>
<td>Configures OSPF to advertise a maximum metric until the router is shut down.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router(config-router)# exit</td>
<td>Exits router configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router(config)# exit</td>
<td>Exits configuration mode and places the router in privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Router# show ip ospf</td>
<td>Displays general information about OSPF routing processes. The <code>show ip ospf</code> command is entered in order to verify that the <code>max-metric router-lsa</code> command has been enabled before the router is shut down or reloaded.</td>
</tr>
</tbody>
</table>

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.

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` for `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` 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 SPF's 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 SPF's 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, Time remaining: 00:01:18
    Condition: on startup for 300 seconds, State: active
    SPF schedule delay 5 secs, Hold time between two SPF's 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
```
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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router# show ip ospf</code></td>
<td>Displays general information about OSPF routing processes and provides information about the configuration settings and status of the OSPF Stub Router Advertisement feature.</td>
</tr>
</tbody>
</table>
Command | Purpose
--- | ---
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, page 54
- Example Advertisement Until Routing Tables Converge, page 54
- Example Graceful Shutdown, page 54

#### 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)# exit
Router(config)# exit
Router# show ip ospf

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>&quot;Configuring OSPF&quot;</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
<tr>
<td>Cisco IOS master command list, all releases</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3137</td>
<td>OSPF Stub Router Advertisement</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

### Table 2  Feature Information for OSPF Stub Router Advertisement

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| OSPF Stub Router Advertisement| 12.1(8)E 12.0(15)S 12.0(15)SC 12.0(16)ST 12.2(4)T 12.2(4)T3 12.2(14)S Cisco IOS XE 3.1.0 SG | 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 |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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, page 57
• Restrictions on OSPF Update Packet-Pacing Configurable Timers, page 57
• Information About OSPF Update Packet-Pacing Configurable Timers, page 58
• Supported Platforms, page 58
• How to Configure OSPF Packet-Pacing Timers, page 59
• Configuration Examples of OSPF Update Packet-Pacing, page 62
• Additional References, page 62
• Feature Information for OSPF Update Packet-Pacing Configurable Timers, page 64

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 associated with changing the default timer values.
Information About OSPF Update Packet-Pacing Configurable Timers

- Functionality of the OSPF Update Packet-Pacing Timers, page 58
- Benefits of OSPF Update Packet-Pacing Configurable Timers, page 58
- Related Features and Technologies, page 58

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 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 used for group LSA refreshment; however, this timer does not change the frequency that individual LSAs are refreshed (the default refresh occurs every 30 minutes).

Note

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.

Related Features and Technologies

The OSPF Update Packet-Pacing Configurable Timers feature is an extension of the OSPF routing protocol. For more information about configuring OSPF, packet pacing, area border router (ABR) and autonomous system boundary router (ASBR) summarization, and stub router configuration, refer to the "Configuring OSPF" module of the Cisco IOS IP Routing Configuration Guide and the Cisco IOS IP Routing: OSPF Command Reference.

Supported Platforms

The OSPF Update Packet-Pacing Configurable Timers feature is supported by the following platforms in Cisco IOS Release 12.2(14)S that support OSPF:

- Cisco 7200 series
Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

How to Configure OSPF Packet-Pacing Timers

See the following sections for configuration tasks for the OSPF Update Packet-Pacing Configurable Timers feature. Each task in the list is identified as either required or optional:

- Configuring OSPF Packet-Pacing Timers, page 59
- Configuring a Group Packet Pacing Timer, page 60
- Verifying OSPF Packet-Pacing Timers, page 61
- Monitoring and Maintaining OSPF Packet-Pacing Timers, page 61

Configuring OSPF Packet-Pacing Timers

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td></td>
</tr>
<tr>
<td>Router(config)# router ospf process-id</td>
<td>Places the router in router configuration mode and enables an OSPF routing process.</td>
</tr>
</tbody>
</table>
Configuring a Group Packet Pacing Timer

To configure a retransmission 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Place the router in router configuration mode and enables an OSPF routing process.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure an LSA group packet pacing timer delay (in seconds).</td>
</tr>
</tbody>
</table>

**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 example output is from the `show ip ospf` command:

```none
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 SPF calculations 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 0x29BEF
  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
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 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

Troubleshooting Tips

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

Monitoring and Maintaining OSPF Packet-Pacing Timers

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# show ip ospf</td>
<td>Displays general information about OSPF routing processes.</td>
</tr>
</tbody>
</table>
### Command and Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>router# show ip ospf neighbor</td>
<td>Displays OSPF neighbor information on a per-interface basis.</td>
</tr>
<tr>
<td>Router# clear ip ospf redistribution</td>
<td>Clears route redistribution based on the OSPF routing process ID.</td>
</tr>
</tbody>
</table>

---

### Configuration Examples of OSPF Update Packet-Pacing

- [Example Flood Pacing](#), page 62
- [Example Retransmission Pacing](#), page 62
- [Example Group Pacing](#), page 62

#### Example 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 Retransmission Pacing

The following example configures 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 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

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>Configuring OSPF</td>
</tr>
</tbody>
</table>

---

*IP Routing: OSPF Configuration Guide, Cisco IOS Release 12.2SR*
### Related Topic

<table>
<thead>
<tr>
<th>OSPF commands</th>
<th><em>Cisco IOS IP Routing: OSPF Command Reference</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS master command list, all releases</td>
<td><em>Cisco IOS Master Command List, All Releases</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Update Packet-Pacing Configurable Timers</td>
<td>12.2(4)T 12.2(4)T3 12.2(8)T</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>12.2(8)T1 12.2(14)S Cisco IOS</td>
<td>• timers pacing flood</td>
</tr>
<tr>
<td></td>
<td>XE 3.1.0 SG</td>
<td>• timers pacing lsa-group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• timers pacing retransmission</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• show ip ospf</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Support for MPLS VPN

Feature History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(8)T</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>

This module 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, page 65
- Feature Overview, page 65
- Supported Platforms, page 71
- Supported Standards MIBs and RFCs, page 72
- Prerequisites, page 73
- Configuration Tasks, page 73
- Monitoring and Maintaining a Sham-Link, page 75
- Configuration Examples, page 75
- Glossary, page 76

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.

Feature Overview

- Using OSPF in PE-CE Router Connections, page 66
- Using a Sham-Link to Correct OSPF Backdoor Routing, page 66
- Sham-Link Configuration Example, page 69
- Benefits, page 71
- Restrictions, page 71
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 that 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 "MPLS Virtual Private Networks Configuration" module.

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, internal
      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, internal
      Extended Community: RT:1:793 OSPF DOMAIN ID:0.0.0.100 OSPF
      RT:1:2:0 OSPF 2
```

OSPF Sham-Link Support for MPLS VPN

Feature Overview
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.

The section, “Creating a Sham-Link, page 73”, describes how to configure a sham-link between two PE routers. For more information about how to configure OSPF, refer to the “Configuring OSPF” module.

**Sham-Link Configuration Example**

The example in this section 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 example 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 above.

```
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
```
The next example 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.

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 example, 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).
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.

**Benefits**

**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.

**Restrictions**
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.

**Related Features and Technologies**
- MPLS
- OSPF
- BGP

**Related Documents**
- *Cisco IOS IP Routing: OSPF Command Reference*
- "MPLS Virtual Private Networks" module
- "Configuring OSPF" module
- *Cisco IOS IP Routing: BGP Configuration Guide, Release 15.0*
- 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

**Supported Platforms**
- Cisco 1400 series
Cisco 1600
Cisco 1600R
Cisco 1710
Cisco 1720
Cisco 1721
Cisco 1750
Cisco 1751
Cisco 2420
Cisco 2600
Cisco 2691
Cisco 3620
Cisco 3631
Cisco 3640
Cisco 3660
Cisco 3725
Cisco 3745
Cisco 7100
Cisco 7200
Cisco 7500
Cisco 7700
URM
Cisco uBR7200

Determining Platform Support Through Cisco Feature Navigator
Cisco IOS software is packaged in feature sets that support specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Supported Standards MIBs and RFCs

Standards
No new or modified standards are supported by this feature.

MIBs
No new or modified MIBs are supported by this feature.
To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

**RFCs**

No new or modified RFCs are supported by this feature.

---

**Prerequisites**

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.

For more information on these OSPF configuration procedures, go to:

---

**Configuration Tasks**

See the following sections for configuration tasks for the sham-link feature. Each task in the list is identified as either required or optional.

- Creating a Sham-Link, page 73 (required)
- Verifying Sham-Link Creation, page 75 (optional)

---

**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.
### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Router1# configure terminal</td>
<td>Enters global configuration mode on the first PE router.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Router1(config)# interface loopback interface-number</td>
<td>Creates a loopback interface to be used as an endpoint of the sham-link on PE-1 and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong> Router1(config-if)# ip vrf forwarding vrf-name</td>
<td>Associates the loopback interface with a VRF. Removes the IP address.</td>
</tr>
<tr>
<td><strong>Step 4</strong> Router1(config-if)# ip address ip-address mask</td>
<td>Reconfigures the IP address of the loopback interface on PE-1.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Router1(config)# end</td>
<td>Returns to EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> Router2# configure terminal</td>
<td>Enters global configuration mode on the second PE router.</td>
</tr>
<tr>
<td><strong>Step 7</strong> Router2(config)# interface loopback interface-number</td>
<td>Creates a loopback interface to be used as the endpoint of the sham-link on PE-2 and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> Router2(config-if)# ip vrf forwarding vrf-name</td>
<td>Associates the second loopback interface with a VRF. Removes the IP address.</td>
</tr>
<tr>
<td><strong>Step 9</strong> Router2(config-if)# ip address ip-address mask</td>
<td>Reconfigures the IP address of the loopback interface on PE-2.</td>
</tr>
<tr>
<td><strong>Step 10</strong> Router1(config)# end</td>
<td>Returns to EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 11</strong> Router1(config)# router ospf process-id vrf vrf-name</td>
<td>Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-1 and enters interface configuration mode.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Router1(config-if)# <strong>area</strong> <strong>area-id sham-link</strong> source-address destination-address cost number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>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. <strong>cost number</strong> configures the OSPF cost for sending an IP packet on the PE-1 sham-link interface.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Router2(config)# <strong>router ospf</strong> process-id <strong>vrf</strong> <strong>vrf-name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Configures the specified OSPF process with the VRF associated with the sham-link interface on PE-2 and enters interface configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th>Router2(config-if)# <strong>area</strong> <strong>area-id sham-link</strong> source-address destination-address cost number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>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. <strong>cost number</strong> configures the OSPF cost for sending an IP packet on the PE-2 sham-link interface.</td>
</tr>
</tbody>
</table>

### 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:

```
Router1# 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router# <strong>show ip ospf sham-links</strong></td>
<td>Displays the operational status of all sham-links configured for a router.</td>
</tr>
<tr>
<td>Router# <strong>show ip ospf data router</strong> <strong>ip-address</strong></td>
<td>Displays information about how the sham-link is advertised as an unnumbered point-to-point connection between two PE routers.</td>
</tr>
</tbody>
</table>

### Configuration Examples

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

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.

OSPF --Open Shortest Path First protocol.

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.

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 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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the Feature Information for OSPF Sham-Link MIB Support, page 91.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

• Finding Feature Information, page 79
• Prerequisites for OSPF Sham-Link MIB Support, page 80
• Restrictions for OSPF Sham-Link MIB Support, page 80
• Information About OSPF Sham-Link MIB Support, page 80
• How to Configure OSPF Sham-Link MIB Support, page 82
• Configuration Examples for OSPF Sham-Link MIB Support, page 88
• Where to Go Next, page 90
• Additional References, page 90
• Command Reference, page 91
• Feature Information for OSPF Sham-Link MIB Support, page 91

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 Open Shortest Path First (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, page 80
- Cisco OSPF MIB and Cisco OSPF Trap MIB Enhancements, page 80

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 between 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, refer the OSPF Sham-Link Support for MPLS VPN feature at the following URL:


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) for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, 12.2(31)SB2, and 12.2(33)SXH. New CLI has 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. The following sections describe the enhancements:

- OSPF Sham-Link Configuration Support, page 80
- OSPF Sham-Link Neighbor Support, page 81
- OSPF Sham-Link Interface Transition State Change Support, page 81
- OSPF Sham-Link Neighbor Transition State Change Support, page 81
- Sham-Link Errors, page 82

OSPF Sham-Link Configuration Support

The cospfShamLinksTable table object stores information about the sham-links that have been configured for the OSPF area. Beginning with Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, 12.2(31)SB2,
and 12.2(33)SXH, the `cospfShamLinksTable` replaces the `cospfShamLinkTable`. 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 object replaces the original `cospfShamLinkStateChange` trap object for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2. 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`

**Note**

The `cospfShamLinkAuthFailure` trap will not be generated because Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2 do not yet support authentication over sham-links. The `cospfShamLinkRxBadPacket` trap will not be generated because it also is not supported by Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2. However, the information can be retrieved from the existing OSPF bad packet traps.

### How to Configure OSPF Sham-Link MIB Support

- **Configuring the Router to Send SNMP Notifications**, page 82
- **Enabling OSPF Sham-Link Error Traps**, page 84
- **Enabling OSPF Sham-Link Retransmissions Traps**, page 85
- **Enabling OSPF Sham-Link State Change Traps**, page 86
- **Verifying OSPF Sham-Link MIB Traps on the Router**, page 88

### Configuring the Router to Send SNMP Notifications

Perform this task to enable the router to send SNMP notifications (traps or informs) defined in the OSPF MIBs. SNMP notifications can be configured on the router and GET operations can be performed from an external management station only after MIB support is enabled.

- **OSPF Configuration Error Notifications**, page 82

**OSPF Configuration Error Notifications**
To enable the sending of OSPF configuration errors notifications, enable the following traps:

- cospfShamLinkConfigError
- cospfShamLinkAuthFailure
- cospfShamLinkRxBadPacket

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> show running-config</td>
<td>Displays the running configuration to determine if an SNMP agent is already running.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• If no SNMP information is displayed, continue with the next step.</td>
</tr>
<tr>
<td>Router# show running-config</td>
<td>If any SNMP information is displayed, you can modify the information or change it as needed.</td>
</tr>
<tr>
<td><strong>Step 3</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server host hostname</td>
<td>Specifies a recipient (target host) for SNMP notification operations.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• If no notification-type is specified, all enabled notifications (traps or informs) will be sent to the specified host.</td>
</tr>
<tr>
<td>Router(config)# snmp-server host 172.20.2.162 version 2c public ospf</td>
<td>• 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.)</td>
</tr>
</tbody>
</table>
### Enabling OSPF Sham-Link Error Traps

Notifications are sent when OSPF sham-link configuration errors are detected. To enable the sending of sham-link configuration error notifications, enable the following `cospfShamLinkConfigError` trap.

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

| Step 3 | snmp-server enable traps ospf cisco-specific errors config-error |

**Example:**

```bash
Router(config)# snmp-server enable traps ospf cisco-specific errors config-error
```

**Purpose:** 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:**

```bash
Router(config)# snmp-server enable traps ospf cisco-specific errors shamlink
```

**Purpose:** 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:**

```bash
Router(config)# end
```

**Purpose:** Ends your configuration session and exits global configuration mode.

### Enabling OSPF Sham-Link Retransmissions Traps

Notifications are sent when OSPF packets retransmissions across a sham-link are detected. To enable the sending of sham-link packet retransmission notifications, enable the following `cospfShamLinkTxRetransmit` trap.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
4. `end`
Enabling OSPF Sham-Link State Change Traps

Notifications are sent when sham-link interface and neighbor state changes are detected. To enable the sending of sham-link state changes notifications, you can enable the following cospfShamLinksStateChange trap, which replaces the original cospfShamLinkStateChange trap, as well as the cospfShamLinkNbrStateChange trap, which is new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2:

- cospfShamLinksStateChange
- cospfShamLinkNbrStateChange

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server enable traps ospf cisco-specific state-change [nssa-trans-change</td>
<td>shamlink [interface</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# snmp-server enable traps ospf cisco-specific state-change</td>
<td>• The neighbor keyword enables the OSPF sham-link neighbor state change traps.</td>
</tr>
<tr>
<td></td>
<td>• The interface keyword enables the OSPF sham-link interface state change traps.</td>
</tr>
<tr>
<td></td>
<td>• The interface-old keyword enables the original OSPF sham-link interface state change trap that is replaced by the cospfShamLinksStateChange and cospfShamLinkNbrStateChange traps for Cisco IOS Releases 12.0(30)S and 12.3(14)T.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> 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.</td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Ends your configuration session and exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Verifying OSPF Sham-Link MIB Traps on the Router

This task verifies that you have enabled OSPF sham-link MIB support.

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show running-config</td>
<td>include traps</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show running-config</td>
<td>include traps</td>
</tr>
</tbody>
</table>

**Configuration Examples for OSPF Sham-Link MIB Support**

- Enabling and Verifying OSPF Sham-Link Error Traps Example, page 88
- Enabling and Verifying OSPF State Change Traps Example, page 89
- Enabling and Verifying OSPF Sham-Link Retransmissions Traps Example, page 89

**Enabling and Verifying OSPF Sham-Link Error Traps Example**

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.
```

### Enabling and Verifying OSPF State Change Traps Example

The following example enables all Cisco-specific OSPF state change traps including the `cospfShamLinksStateChange` and `cospfShamLinkNbrStateChange` traps that are new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2:

```
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 that is new for Cisco IOS Releases 12.0(30)S, 12.3(14)T, 12.2(33)SRA, and 12.2(31)SB2.

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
```

### Enabling and Verifying OSPF Sham-Link Retransmissions Traps Example

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 Network Management Configuration Guide*.

**Additional References**

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

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF sham-links</td>
<td>OSPF Sham-Link Support for MPLS VPN</td>
</tr>
<tr>
<td>SNMP configuration</td>
<td><em>Cisco IOS Network Management Configuration Guide</em></td>
</tr>
<tr>
<td>SNMP commands</td>
<td><em>Cisco IOS Network Management Command Reference</em></td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

**MIBs**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-OSPF-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td>• CISCO-OSPF-TRAP-MIB</td>
<td>and feature sets, use Cisco MIB Locator found at the following URL:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

**RFCs**

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the Cisco IOS IP Routing: OSPF Command Reference. For information about all Cisco IOS commands, go to the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or to the Cisco IOS Master Commands List.

- `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`

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 4 Feature Information for OSPF Sham-Link MIB Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Sham-Link MIB Support</td>
<td>12.0(30)S 12.3(14)T 12.2(33)SRA 12.2(31)SB2 12.2(33)SXH</td>
<td>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.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Support for Multi-VRF on CE Routers

The OSPF Support for Multi-VRF on CE Routers feature provides the capability of suppressing 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 forward (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, page 93
- Information About OSPF Support for Multi-VRF on CE Routers, page 93
- How to Configure OSPF Support for Multi-VRF on CE Routers, page 94
- Configuration Examples for OSPF Support for Multi-VRF on CE Routers, page 95
- Additional References, page 97
- Feature Information for OSPF Support for Multi-VRF on CE Routers, page 98
- Glossary, page 98

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 of suppressing 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 forward (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

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

- Configuring the Multi-VRF Capability for OSPF Routing, page 94
- Verifying the OSPF Multi-VRF Configuration, page 95

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. router ospf process-id [vrf vpn-name]
5. capability vrf-lite

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enables OSPF routing and enters router configuration mode.</td>
</tr>
<tr>
<td>Step 2 show ip ospf [process-id]</td>
<td>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.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; show ip ospf 1</td>
<td></td>
</tr>
<tr>
<td>Step 3 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 4 router ospf process-id [vrf vpn-name]</td>
<td>Enables OSPF routing and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# router ospf 1 vrf grc</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 5** capability vrf-lite | Applies the multi-VRF capability to the OSPF process.

**Example:**

```
Router(config)# capability vrf-lite
```

---

### 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 151.1.1.1 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Connected to MPLS VPN Superbackbone
SPF schedule delay 5 secs, Hold time between two SPF's 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 Examples for OSPF Support for Multi-VRF on CE Routers

- Example Configuring the Multi-VRF Capability, page 95
- Example Verifying the OSPF Multi-VRF Configuration, page 96

---

### 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
  ip vrf forwarding grc
  ip address 192.168.1.1 255.255.255.252
```
interface Serial3/0
  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
O IA 192.168.192.0/24 [110/138] via 192.168.1.9, 00:06:08, Serial3/0
O IA 192.168.193.0/24 [110/148] via 192.168.1.13, 00:06:08, Serial2/0
O IA 192.168.193.0/24 [110/148] via 192.168.1.9, 00:06:08, Serial3/0
O IA 192.168.128.0/24 [110/74] via 192.168.1.13, 00:06:08, Serial2/0
O IA 192.168.128.0/24 [110/74] via 192.168.1.9, 00:06:08, Serial3/0
O IA 192.168.129.0/24 [110/84] via 192.168.1.13, 00:06:08, Serial2/0
O IA 192.168.129.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0
O IA 192.168.130.0/24 [110/84] via 192.168.1.13, 00:06:08, Serial2/0
O IA 192.168.130.0/24 [110/84] via 192.168.1.9, 00:06:08, Serial3/0
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
O E2 172.16.10.0 [110/5] via 192.168.1.13, 00:06:08, Serial2/0
O IA 192.168.131.0/24 [110/94] via 192.168.1.13, 00:06:20, Serial2/0
O IA 192.168.131.0/24 [110/94] via 192.168.1.9, 00:06:20, Serial3/0
192.168.1.0/30 is subnetted, 4 subnets
C 192.168.1.0 is directly connected, Serial3/0
C 192.168.1.12 is directly connected, Serial2/0
O 192.168.1.0 [110/128] via 192.168.1.13, 00:06:20, Serial2/0
O 192.168.1.0 [110/128] via 192.168.1.13, 00:06:20, Serial3/0

Example Verifying the OSPF Multi-VRF Configuration

This example illustrates the output display from the show ip ospf process command after OSPF multi-VRF has been configured on the router.

Router# show ip ospf database external 172.16.0.0 self
OSPF Router with ID (10.0.0.1) (Process ID 100)
  Type-5 AS External Link States
  LS age: 175
  Options: (No TOS-capability, DC)
  LS Type: AS External Link
  Link State ID: 172.16.0.0 (External Network Number)
  Advertising Router: 10.0.0.1
  LS Seq Number: 80000001
  Checksum: 0xEA9E
  Length: 36
  Network Mask: /8
  Metric Type: 2 (Larger than any link state path)
  MTID: 0
  Metric: 20
  Forward Address: 0.0.0.0
  External Route Tag: 0
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>Multiprotocol Label Switching (MPLS)</td>
<td>MPLS Multi-VRF (VRF Lite) Support</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| OSPF Support for Multi-VRF on CE Routers | 12.0(21)ST 12.0(22)S 12.2(8)B 12.2(13)T 12.2(14)S Cisco IOS XE 3.1.0 SG | The OSPF Support for Multi-VRF on CE Routers feature provides the capability to suppress provider edge (PE) checks that are needed to prevent loops when the PE is performing a mutual redistribution of packets between the OSPF and BGP protocols. When VPN routing and forwarding (VRF) is used on a router that is not a PE (that is, one that is not running BGP), the checks can be turned off to allow for correct population of the VRF routing table with routes to IP prefixes. The following commands are introduced or modified in the feature documented in this module:  
  - capability vrf-lite |

Glossary

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

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

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

**LSA** --link-state advertisement. Broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.
**PE Router** -- Provider Edge router, an edge router in the P network, defined as a P router which attaches directly to a C router.

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

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

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

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

**VRF** -- VPN Routing and Forwarding.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Forwarding Address Suppression in Translated Type-5 LSAs

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

- Finding Feature Information, page 101
- Prerequisites for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 101
- Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 102
- How to Suppress OSPF Forwarding Address in Translated Type-5 LSAs, page 103
- Configuration Examples for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 104
- Additional References, page 105
- Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 106

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 in Translated Type-5 LSAs

This document presumes you have OSPF configured on the networking device; it does not document other steps to configure OSPF.
Information About OSPF Forwarding Address Suppression in Translated Type-5 LSAs

- Benefits of OSPF Forwarding Address Suppression in Translated Type-5 LSAs, page 102
- When to Suppress OSPF Forwarding Address in Translated Type-5 LSAs, page 102

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

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

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

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

Figure 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 OSPF Forwarding Address in Translated Type-5 LSAs

- Suppressing OSPF Forwarding Address in Translated Type-5 LSAs, page 103

### Suppressing OSPF Forwarding Address in Translated Type-5 LSAs

---

**Caution**

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

---

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>
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 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 in Translated Type-5 LSAs**

- Example Suppressing OSPF Forwarding Address in Translated Type-5 LSAs, page 104

**Example Suppressing OSPF Forwarding Address in Translated Type-5 LSAs**

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

```plaintext
interface ethernet 0
 ip address 10.93.1.1 255.255.255.0
 ip ospf cost 1
 interface ethernet 1
 ip address 10.94.1.1 255.255.255.0
 router ospf 1
 network 10.93.0.0 0.0.255.255 area 0.0.0.0
 network 10.94.0.0 0.0.255.255 area 10
 area 10 nssa translate type7 suppress-fa
```
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes the router to be noncompliant with RFC 1587.</td>
<td><em>The OSPF NSSA Option</em></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for OSPF Forwarding Address Suppression in Translated Type-5 LSAs

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

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| OSPF Forwarding Address Suppression in Translated Type-5 LSAs               | 12.2(15)T 12.2(18)S       | The OSPF Forwarding Address Suppression in Translated Type-5 LSAs feature causes a not-so-stubby area (NSSA) area border router (ABR) to translate Type-7 link state advertisements (LSAs) to Type-5 LSAs, but to use the address 0.0.0.0 for the forwarding address instead of that specified in the Type-7 LSA. This feature causes routers that are configured not to advertise forwarding addresses into the backbone to direct forwarded traffic to the translating NSSA ABRs. The following commands are introduced or modified:  
  • area nssa translate  
  • show ip ospf |
|                                                                             | 12.2(27)SBC Cisco IOS XE 3.1.0 SG |                                                                                                                                                      |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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, page 107
• Prerequisites for OSPF Inbound Filtering Using Route Maps with a Distribute List, page 107
• Information About OSPF Inbound Filtering Using Route Maps with a Distribute List, page 107
• How to Configure OSPF Inbound Filtering Using Route Maps, page 109
• Configuration Examples for OSPF Inbound Filtering Using Route Maps with a Distribute List, page 110
• Additional References, page 111
• Feature Information for OSPF Inbound Filtering Using Route Maps with a Distribute List, page 112

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 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

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

---

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

• Configuring OSPF Route Map-Based Filtering, page 109

Configuring OSPF Route Map-Based Filtering

**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.
6. exit
7. router ospf process-id
8. distribute-list route-map map-tag in
9. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2** configure terminal |

| **Example:** | |
| Router# configure terminal | |

**Step 3** route-map map-tag [permit | deny] [sequence-number] |

<p>| <strong>Example:</strong> | |
| Router(config)# route-map tag-filter deny 10 | Defines a route map to control filtering. |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong> match tag <em>tag-name</em></td>
<td>Matches routes with a specified name, to be used as the route map is referenced.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# match tag 777</td>
<td>• At least one <em>match</em> command is required, but it need not be this <em>match</em> command. This is just an example.</td>
</tr>
<tr>
<td></td>
<td>• The list of <em>match</em> commands available to be used in this type of route map appears on the <em>distribute-list in</em> command reference page.</td>
</tr>
<tr>
<td></td>
<td>• This type of route map will have no <em>set</em> commands.</td>
</tr>
<tr>
<td><strong>Step 5</strong> Repeat Steps 3 and 4 with other <em>route-map</em> and <em>match</em> commands.</td>
<td>Optional.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Exits router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> router ospf <em>process-id</em></td>
<td>Configures an OSPF routing process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# router ospf 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> distribute-list route-map <em>map-tag in</em></td>
<td>Enables filtering based on an OSPF route map.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# distribute-list route-map tag-filter in</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> end</td>
<td>Exits router configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# end</td>
<td></td>
</tr>
</tbody>
</table>

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

- Example OSPF Route Map-Based Filtering, page 111
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.

```plaintext
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

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Inbound Filtering Using Route Maps with a Distribute List</td>
<td>12.0(24)S 12.2(15)T 12.2(18)S 12.2(27)SBC Cisco IOS XE 3.1.0 SG</td>
<td>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. The following command was introduced or modified: distribute-list in (IP).</td>
</tr>
</tbody>
</table>
OSPF Inbound Filtering Using Route Maps with a Distribute List

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Shortest Path First Throttling

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. 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 network topology is unstable, SPF throttling calculates SPF scheduling intervals to be longer until topology becomes stable.

Feature Specifications for OSPF Shortest Path First Throttling

<table>
<thead>
<tr>
<th>Feature History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
</tr>
<tr>
<td>12.2(14)S</td>
</tr>
<tr>
<td>12.0(23)S</td>
</tr>
<tr>
<td>12.2(15)T</td>
</tr>
</tbody>
</table>

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

- Finding Feature Information, page 115
- Information About OSPF SPF Throttling, page 116
- How to Configure OSPF SPF Throttling, page 117
- Configuration Examples for OSPF SPF Throttling, page 120
- Additional References, page 120

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

- Shortest Path First Calculations, page 116

Shortest Path First Calculations

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 Topology Change Event**
How to Configure OSPF SPF Throttling

- Configuring OSPF SPF Throttling, page 117
- Verifying SPF Throttle Values, page 118

Configuring OSPF SPF Throttling

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot / port`
4. `ip address ip-address mask [secondary]`
5. `exit`
6. `router ospf process-id`
7. `network network-number [mask | prefix-length]`
8. `timers throttle spf spf-start spf-hold spf-max-wait`
9. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot / port</td>
<td>Enters interface configuration mode for the interface specified.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface ethernet 1/1/1</td>
<td></td>
</tr>
</tbody>
</table>
Command or Action | Purpose
--- | ---
**Step 4** ip address ip-address mask [secondary] | Sets a primary or secondary IP address for an interface.

**Example:**

Router(config-if)# ip address 192.168.0.2 255.255.255.0

**Step 5** exit | Exits interface configuration mode.

**Example:**

router# exit

**Step 6** router ospf process-id | Configures an OSPF routing process.

**Example:**

Router(config)# router ospf 1

**Step 7** network network-number [mask | prefix-length] | Configures the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP Server.

**Example:**

Router(config-router)# network 192.168.0.0 0.0.255.255 area 0

**Step 8** timers throttle spf spf-start spf-hold spf-max-wait | Sets OSPF throttling timers.

**Example:**

Router(config-router)# timers throttle spf 10 4800 90000

**Step 9** end | Exits configuration mode.

**Example:**

Router(config-router)# end

---

**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...."
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 SPF's 1000 msecs
Maximum wait time between two consecutive SPF's 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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process &quot;ospf 201&quot; with ID 192.42.110.200</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports ...</td>
<td>Number of types of service supported (Type 0 only).</td>
</tr>
<tr>
<td>It is ...</td>
<td>Possible types are internal, area border, or autonomous system boundary.</td>
</tr>
<tr>
<td>Summary Link update interval</td>
<td>Specifies summary update interval in hours:minutes:seconds, and time until next update.</td>
</tr>
<tr>
<td>External Link update interval</td>
<td>Specifies external update interval in hours:minutes:seconds, and time until next update.</td>
</tr>
<tr>
<td>Redistributing External Routes from</td>
<td>Lists of redistributed routes, by protocol.</td>
</tr>
<tr>
<td>SPF calculations</td>
<td>Lists start, hold, and maximum wait interval values in milliseconds.</td>
</tr>
<tr>
<td>Number of areas</td>
<td>Number of areas in router, area addresses, and so on.</td>
</tr>
<tr>
<td>SPF algorithm last executed</td>
<td>Shows the last time an SPF calculation was performed in response to topology change event records.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Link State Update Interval</td>
<td>Specifies router and network link-state update interval in hours:minutes:seconds, and time until next update.</td>
</tr>
<tr>
<td>Link State Age Interval</td>
<td>Specifies max-aged update deletion interval, and time until next database cleanup, in hours:minutes:seconds.</td>
</tr>
</tbody>
</table>

### Configuration Examples for OSPF SPF Throttling

- Throttle Timers Example, page 120

#### Throttle Timers Example

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.

```plaintext
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 0
```

### Additional References

For additional information related to OSPF, refer to the following references:

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
<tr>
<td>OSPF configuration tasks</td>
<td>&quot;Configuring OSPF&quot; module in the <em>Cisco IOS IP Routing Protocols Configuration Guide</em></td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
</tr>
</tbody>
</table>
### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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 would result in faster convergence in an Open Shortest Path First (OSPF) network.

• Finding Feature Information, page 123
• Prerequisites for OSPF Support for Fast Hello Packets, page 123
• Information About OSPF Support for Fast Hello Packets, page 123
• How to Configure OSPF Fast Hello Packets, page 124
• Configuration Examples for OSPF Support for Fast Hello Packets, page 126
• Additional References, page 126
• Feature Information for OSPF Support for Fast Hello Packets, page 127

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 configured in the network already or 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, page 124
• OSPF Fast Hello Packets, page 124
• Benefits of OSPF Fast Hello Packets, page 124
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 124.

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 sent 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 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 125
### 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables higher privilege levels, such as privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong> <code>interface type number</code></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface ethernet 0</td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>ip ospf dead-interval minimal hello-multiplier multiplier</code></td>
<td>Sets the interval during which at least one hello packet must be received, or else the neighbor is considered down.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# ip ospf dead-interval minimal hello-multiplier 5</td>
</tr>
<tr>
<td><strong>Step 5</strong> <code>end</code></td>
<td>(Optional) Saves configuration commands to the running configuration file, exits configuration mode, and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>

- In the example, OSPF Support for Fast Hello Packets is enabled by specifying the `minimal` keyword and the `hello-multiplier` keyword and value. Because the multiplier is set to 5, five hello packets will be sent every second.
Command or Action | Purpose
--- | ---
**Step 6** `show ip ospf interface [interface-type interface-number]` | (Optional) Displays OSPF-related interface information.  
- The relevant fields that verify OSPF fast hello packets are indicated in the sample output following this table.

**Example:**

`Router# show ip ospf interface ethernet 1/3`
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Support for Fast Hello Packets</td>
<td>12.0(23)S 12.2(18)S 12.2(27)SBC 12.2(15)T</td>
<td>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 would result in faster convergence in an Open Shortest Path First (OSPF) network. The following command was introduced: <code>ip ospf dead-interval</code>.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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.

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 for OSPF Incremental SPF, page 132.

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

• Finding Feature Information, page 129
• Prerequisites for OSPF Incremental SPF, page 129
• Information About OSPF Incremental SPF, page 129
• How to Enable OSPF Incremental SPF, page 130
• Configuration Examples for OSPF Incremental SPF, page 131
• Additional References, page 131
• Feature Information for OSPF Incremental SPF, page 132

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, page 130**

**Enabling Incremental SPF**

This section describes how to enable incremental SPF.

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code> Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router&gt; enable</code> Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code> Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td><code>Router# configure terminal</code></td>
</tr>
</tbody>
</table>
### Step 3

**router ospf** `process-id`

Configures an OSPF routing process.

**Example:**

```
Router(config)# router ospf 1
```

### Step 4

**ispf**

Enables incremental SPF.

**Example:**

```
Router(config-router)# ispf
```

### Step 5

**end**

Exits router configuration mode.

**Example:**

```
Router(config-router)# end
```

## Configuration Examples for OSPF Incremental SPF

- Example Incremental SPF, page 131

## Example Incremental SPF

This example enables incremental SPF:

```
router ospf 1
ispf
```

## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
### Table 10 Feature Information for OSPF Incremental SPF

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Incremental SPF</td>
<td>12.0(24)S 12.3(2)T 12.2(18)S 12.2(27)SBC 12.2(33)SRA 12.2(33)XNE Cisco IOS XE 3.1.0 SG</td>
<td>OSPF can be configured to use an incremental SPF algorithm for calculating the shortest path first routes. Incremental SPF is slightly 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</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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, page 135
- Prerequisites for OSPF Limit on Number of Redistributed Routes, page 135
- Information About OSPF Limit on Number of Redistributed Routes, page 135
- How to Configure OSPF Limit the Number of OSPF Redistributed Routes, page 136
- Configuration Examples for OSPF Limit on Number of Redistributed Routes, page 139
- Additional References, page 140
- Feature Information for OSPF Limit on Number of Redistributed Routes, page 141

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 Configure OSPF 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 OSPF Redistributed Routes, page 136
- Requesting a Warning About the Number of Routes Redistributed into OSPF, page 138

Limiting the Number of OSPF Redistributed Routes

This task describes how to limit the number of OSPF redistributed routes. If the number of redistributed routes reaches the maximum value configured, no more routes will be redistributed.

The redistribution limit applies to all IP redistributed prefixes, including summarized ones. The redistribution limit does not apply to default routes or prefixes that are generated as a result of Type-7 to Type-5 translation.

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> router ospf <em>process-id</em></td>
<td>Configures an OSPF routing process.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# router ospf 1</td>
<td></td>
</tr>
</tbody>
</table>

| **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] | Redistributes routes from one routing domain into another routing domain. |
| Example: | |
| Router(config-router)# redistribute eigrp 10 | |

| **Step 5** redistribute maximum-prefix *maximum* [threshold] | Sets a maximum number of IP prefixes that are allowed to be redistributed into OSPF. |
| Example: | |
| Router(config-router)# redistribute maximum-prefix 100 80 | |

- 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 | Exits router configuration mode. |
| Example: | |
| Router(config-router)# end | |

| **Step 7** show ip ospf [process-id] | (Optional) Displays general information about OSPF routing processes. |
| Example: | |
| Router# show ip ospf 1 | |

- 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

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
• Enter your password if prompted. |
| **Example:** | Router> enable |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** | Router# configure terminal |
| **Step 3** router ospf process-id | Configures an OSPF routing process. |
| **Example:** | Router(config)# router ospf 1 |
| **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] | Redistributes routes from one routing domain into another routing domain.  
**Note** The redistribution count applies to external IP prefixes, including summarized routes. Default routes and prefixes that are generated as a result of Type-7 to Type-5 translation are not considered. |
| **Example:** | Router(config-router)# redistribute eigrp 10 |
**Step 5** redistribute maximum-prefix *maximum*  
*threshold*  
**Purpose**

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.

**Example:**

```
Router(config-router)# redistribute maximum-prefix 1000 80 warning-only
```

**Step 6** end  
**Purpose**

Exits router configuration mode.

**Example:**

```
Router(config-router)# end
```

**Configuration Examples for OSPF Limit on Number of Redistributed Routes**

- [Example OSPF Limit on Number of Redistributed Routes](#), page 139
- [Example Requesting a Warning About the Number of Redistributed Routes](#), page 140

**Example OSPF Limit on 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

<table>
<thead>
<tr>
<th>Related Documents</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standards</td>
</tr>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MIBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIBs</td>
</tr>
<tr>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RFCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFCs</td>
</tr>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| OSPF Limit on Number of Redistributed Routes                                | 12.0(25)S 12.3(2)T 12.2(18)S 12.2(27)SBC Cisco IOS XE 3.1.0 SG | 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 Limit on Number of Redistributed Routes

Feature Information for OSPF Limit on Number of Redistributed Routes
OsPF Limit on Number of Redistributed Routes

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Link-State Advertisement Throttling

The OSPF Link-State Advertisement (LSA) 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 Open Shortest Path First (OSPF) convergence by providing LSA rate limiting in milliseconds.

History for the OSPF LSA Throttling Feature

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(25)S</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>12.3(2)T</td>
<td>This feature was integrated into Cisco IOS Release 12.3(2)T.</td>
</tr>
<tr>
<td>12.2(18)S</td>
<td>This feature was integrated into Cisco IOS Release 12.2(18)S.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This feature was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
</tbody>
</table>

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

- Finding Feature Information, page 143
- Prerequisites for OSPF LSA Throttling, page 144
- Information About OSPF LSA Throttling, page 144
- How to Customize OSPF LSA Throttling, page 144
- Configuration Examples for OSPF LSA Throttling, page 150
- Additional References, page 151

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, page 144
- How OSPF LSA Throttling Works, page 144

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 145
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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> router ospf process-id</td>
<td>Configures an OSPF routing process.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# router ospf 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> timers throttle lsa all start-interval hold-interval max-interval</td>
<td>(Optional) Sets the rate-limiting values (in milliseconds) for LSA generation.</td>
</tr>
<tr>
<td></td>
<td>• The default values are as follows:</td>
</tr>
<tr>
<td></td>
<td>◦ start-interval is 0 milliseconds</td>
</tr>
<tr>
<td></td>
<td>◦ hold-interval is 5000 milliseconds</td>
</tr>
<tr>
<td></td>
<td>◦ max-interval is 5000 milliseconds</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-router)# timers throttle lsa all 100 10000 45000</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 5 | timers lsa arrival milliseconds | (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 | Exits router configuration mode. |
| Step 7 | show ip ospf timers rate-limit | (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. |

#### Example:

**Router(config-router)# timers lsa arrival 2000**

**Router# show ip ospf timers rate-limit**

**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**

---

**OSPF Link-State Advertisement Throttling**

**How to Customize OSPF LSA Throttling**

**IP Routing: OSPF Configuration Guide, Cisco IOS Release 12.2SR**

---

146
### Step 8 show ip ospf

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf</td>
<td>(Optional) Displays information about OSPF.</td>
</tr>
</tbody>
</table>

- The output lines shown in bold in the example indicate the LSA throttling values.

**Example:**

Router# show ip ospf

**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
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Initial LSA throttle delay 100 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Minimum hold time for LSA throttle 10000 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Maximum wait time for LSA throttle 45000 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Minimum LSA arrival 1000 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>LSA group pacing timer 240 secs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Interface flood pacing timer 33 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Retransmission pacing timer 66 msecs</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Number of external LSA 0. Checksum Sum 0x0</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Number of opaque AS LSA 0. Checksum Sum 0x0</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Number of DCbitless external and opaque AS LSA 0</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Number of DoNotAge external and opaque AS LSA 0</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Number of areas in this router is 1. 1 normal 0 stub 0 nssa</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>External flood list length 0</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Area 24</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Number of interfaces in this area is 2</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Area has no authentication</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>SPF algorithm last executed 04:28:18.396 ago</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>SPF algorithm executed 8 times</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Area ranges are</td>
<td></td>
</tr>
</tbody>
</table>
### Configuration Examples for OSPF LSA Throttling

- Example OSPF LSA Throttling, page 150

### 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
OSPF Link-State Advertisement Throttling
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.

### History for the OSPF Support for Unlimited Software VRFs per Provider Edge Router Feature

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.3(4)T</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>12.0(27)S</td>
<td>This feature was integrated into Cisco IOS Release 12.0(27)S.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This feature was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This feature was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This feature was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
</tbody>
</table>

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at [http://www.cisco.com/go/fn](http://www.cisco.com/go/fn). You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

- Finding Feature Information, page 154
- Prerequisites for OSPF Support for Unlimited Software VRFs per PE Router, page 154
- Restrictions for OSPF Support for Unlimited Software VRFs per PE Router, page 154
- Information About OSPF Support for Unlimited Software VRFs per PE Router, page 154
- How to Configure OSPF Support for Unlimited Software VRFs per PE Router, page 154
- Configuration Examples for OSPF Support for Unlimited Software VRFs per PE Router, page 156
- Additional References, page 157
- Glossary, page 158
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. It is a common scenario when OSPF is used as the IGP between a customer edge (CE) router and a PE router. OSPF was not scalable in 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 and Verifying Unlimited Software VRFs per Provider Edge Router, page 155
## Configuring and Verifying Unlimited Software VRFs per Provider Edge Router

### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 `enable`   | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| Example:          | Router> enable |
| Step 2 `configure terminal` | Enters global configuration mode. |
| Example:          | Router# configure terminal |
| Step 3 `router ospf process-id [vrf vpn-name]` | Enables OSPF routing.  
  - The `process-id` argument identifies the OSPF process.  
  - Use the `vrf` keyword and `vpn-name` argument to identify a VPN.  
  - **Note** You now can configure as many OSPF VRF processes as needed. |
| Example:          | Router(config)# router ospf 1 vrf crf-1 |
| Step 4 `end`     | Returns to privileged EXEC mode. |
| Example:          | Router(config-router)# end |
| Step 5 `show ip ospf [process-id]` | Displays general information about OSPF routing processes. |
| Example:          | Router# show ip ospf 1 |
Configuration Examples for OSPF Support for Unlimited Software VRFs per PE Router

- Example Configuring OSPF Support for Unlimited Software VRFs per PE Router, page 156
- Example Verifying OSPF Support for Unlimited Software VRFs per PE Router, page 156

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)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)#
exit
```

Example Verifying OSPF Support for Unlimited Software VRFs per PE Router

This example illustrates the output display from the `show ip ospf` command to verify that the 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
```
### Additional References

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

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td><em>Cisco IOS IP Routing: OSPF Configuration Guide</em></td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
</table>
| 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

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

#### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
**multiprotocol BGP** -- Border Gateway Protocol (BGP) can be used as an interdomain routing protocol in networks that use Connectionless Network Service (CLNS) as the network-layer protocol.
OSPFC 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 software to be compliant with RFC 2328.

- Finding Feature Information, page 159
- Information About OSPF Area Transit Capability, page 159
- How to Disable OSPF Area Transit Capability, page 159
- Additional References, page 160
- Feature Information for OSPF Area Transit Capability, page 161

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

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 forward traffic along those paths rather than using the virtual link or path, which are not as optimal.

For a detailed description of OSPF area transit capability, see RFC 2328, OSPF Version 2, at the following URL:

http://www.faqs.org/rfcs/rfc2328.html

How to Disable OSPF Area Transit Capability

- Disabling OSPF Area Transit Capability on an Area Border Router, page 160
Disabling OSPF Area Transit Capability on an Area Border Router

This task describes how to disable the OSPF Area Transit Capability feature on an OSPF ABR.

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |
| **Step 2** configure terminal | Enters global configuration mode. |
| **Step 3** router ospf process-id [vrf vpn-name] | Enables OSPF routing and enters router configuration mode.  
  - The **process-id** argument identifies the OSPF process. |
| **Step 4** no capability transit | Disables OSPF area capability transit on all areas for a router process. |

**Example:**

**Step 1**

```
Router> enable
```

**Step 2**

```
Router# configure terminal
```

**Step 3**

```
Router(config)# router ospf 100
```

**Step 4**

```
Router(config-router)# no capability transit
```

---

**Additional References**

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>“Configuring OSPF” module</td>
</tr>
</tbody>
</table>

---

*IP Routing: OSPF Configuration Guide, Cisco IOS Release 12.2SR*
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2328</td>
<td>OSPF Version 2</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

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 12  Feature Information for OSPF Area Transit Capability

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| OSPF Area Transit Capability | 12.0(27)S 12.3(7)T 12.2(25)S 12.2(27)SBC 12.2(33)SRA 12.2(33)SXH Cisco IOS XE 3.1.0 SG | 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 software to be compliant with RFC 2328. The following commands are introduced or modified in the feature documented in this module:  
• capability transit |

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.
OSPФ Per-Interface Link-Local Signaling

The OSPФ 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, page 163
- Information About OSPФ Per-Interface Link-Local Signaling, page 163
- How to Configure OSPФ Per-Interface Link-Local Signaling, page 164
- Configuration Examples for OSPФ Per-Interface Link-Local Signaling, page 165
- Additional References, page 167
- Feature Information for OSPФ Per-Interface Link-Local Signaling, page 168

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 OSPФ Per-Interface Link-Local Signaling

- Benefits of the OSPФ Per-Interface Link-Local Signaling Feature, page 163

Benefits of the OSPФ Per-Interface Link-Local Signaling Feature

LLS allows for the extension of existing OSPФ packets in order to provide additional bit space. The additional bit space enables greater information per packet exchange between OSPФ neighbors. This functionality is used, for example, by the OSPФ 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 OSPФ 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 Open Shortest Path First (OSPF) neighbors in the network.

**How to Configure OSPF Per-Interface Link-Local Signaling**

- Turning Off LLS on a Per-Interface Basis, page 164

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1 enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2 configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3 interface type slot/port</strong></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface Ethernet 1/0</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip address ip-address mask [secondary]</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 10.2.145.20 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> no ip directed-broadcast [access-list-number</td>
<td>extended access-list-number]</td>
</tr>
<tr>
<td></td>
<td>• The forwarding of IP directed broadcasts on Ethernet interface 1/0 is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ip ospf message-digest-key key-id encryption-type md5 key</td>
<td>Enables OSPF Message Digest 5 (MD5) algorithm authentication.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip ospf message-digest-key 100 md5 testing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> [no</td>
<td>default] ip ospf lls [disable]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip ospf lls disable</td>
<td></td>
</tr>
</tbody>
</table>

**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 OSPF Per-Interface Link-Local Signaling, page 166
Example OSPF Per-Interface Link-Local Signaling

In the following example, LLS has been enabled on Ethernet interface 1/0 and disabled on Ethernet interface 2/0:

```conf
interface Ethernet1/0
 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 Ethernet2/0
 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 Ethernet interface 1/0 and disabled for interface Ethernet 2/0:

```
Router# show ip ospf interface
Ethernet1/0 is up, line protocol is up
 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)

Ethernet2/0 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)

Ethernet3/0 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>&quot;Configuring OSPF&quot;</td>
</tr>
<tr>
<td>Configuring OSPF NSF Awareness</td>
<td>&quot;NSF-OSPF&quot;</td>
</tr>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OSPF Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2328</td>
<td>OSPF Version 2</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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 13    Feature Information for OSPF Per-Interface Link-Local Signaling

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Per-Interface Link-Local Signaling</td>
<td>12.0(27)S 12.3(7)T</td>
<td>The OSPF Per-Interface Link-Local Signaling feature allows you to selectively enable</td>
</tr>
<tr>
<td></td>
<td>12.2(25)S</td>
<td>or disable Link-Local Signaling (LLS) for a specific interface regardless of the</td>
</tr>
<tr>
<td></td>
<td>12.2(18)SXE</td>
<td>global (router level) setting that you have previously configured.</td>
</tr>
<tr>
<td></td>
<td>12.2(27)SBC</td>
<td>The following command was introduced or modified: ip ospf lls.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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.

**History for the OSPF Link-State Database Overload Protection Feature**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.0(27)S</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>12.3(7)T</td>
<td>This feature was integrated into Cisco IOS Release 12.3(7)T.</td>
</tr>
<tr>
<td>12.2(25)S</td>
<td>This feature was integrated into Cisco IOS Release 12.2(25)S.</td>
</tr>
<tr>
<td>12.2(18)SXE</td>
<td>This feature was integrated into Cisco IOS Release 12.2(18)SXE.</td>
</tr>
<tr>
<td>12.2(27)SBC</td>
<td>This feature was integrated into Cisco IOS Release 12.2(27)SBC.</td>
</tr>
</tbody>
</table>

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at [http://www.cisco.com/go/fn](http://www.cisco.com/go/fn). You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

- Finding Feature Information, page 172
- Prerequisites for OSPF Link-State Database Overload Protection, page 172
- Information About OSPF Link-State Database Overload Protection, page 172
- How to Configure OSPF Link-State Database Overload Protection, page 173
- Configuration Examples for OSPF Link-State Database Overload Protection, page 175
- Additional References, page 176
- Glossary, page 177
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 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 counts 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 NonSelf-Generating LSAs for an OSPF Process, page 173

### Limiting the Number of NonSelf-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*

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 enable     | Enables privileged EXEC mode.  
| Example:          | 
| Router> enable    | • Enter your password if prompted.  
| Step 2 configure terminal | Enters global configuration mode.  
| Example:          | 
| Router# configure terminal |  
| Step 3 router ospf *process-id* | Enables OSPF routing.  
| Example:          | • The *process-id* argument identifies the OSPF process.  
| Router(config)# router ospf 1 |  
|
### Command or Action

<table>
<thead>
<tr>
<th>Step 4 router-id ip-address</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Router(config-router)# router-id 10.0.0.1</td>
<td>Specifies a fixed router ID for an OSPF process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5 log-adjacency-changes [detail]</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Router(config-router)# log-adjacency-changes</td>
<td>Configures the router to send a syslog message when an OSPF neighbor goes up or down.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 6 max-lsa maximum-number [threshold-percentage] [warning-only] [ignore-time minutes] [ignore-count count-number] [reset-time minutes]</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Router(config-router)# max-lsa 12000</td>
<td>Limits the number of nonself-generated LSAs an OSPF routing process can keep in the OSPF link-state database (LSDB).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 7 network ip-address wildcard-mask area area-id</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Router(config-router)# network 209.165.201.1 255.255.255.255 area 0</td>
<td>Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.</td>
</tr>
</tbody>
</table>

- Verifying the Number of Nonself-Generated LSAs on a Router, page 174

### Verifying the Number of Nonself-Generated LSAs on a Router

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 given point in 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
```
Configuration Examples for OSPF Link-State Database Overload Protection

• Example Setting a Limit for LSA Generation, page 175

Example Setting a Limit for LSA Generation

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring OSPF</td>
<td>- &quot;Configuring OSPF&quot; module</td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

#### MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>
OSPF Link-State Database Overload Protection

Glossary

**LSDB** --link-state database.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 Enhanced Traffic Statistics for OSPFv2 and OSPFv3

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

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

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

- Finding Feature Information, page 179
- Prerequisites for OSPF Enhanced Traffic Statistics, page 179
- Information About OSPF Enhanced Traffic Statistics, page 180
- How to Display and Clear OSPF Enhanced Traffic Statistics, page 180
- Configuration Examples for OSPF Enhanced Traffic Commands, page 181
- Additional References, page 185
- Feature Information for OSPF Enhanced Traffic Statistics, page 186

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, page 180
- Displaying and Clearing OSPF Traffic Statistics for OSPFv3, page 181

Displaying and Clearing OSPF Traffic Statistics for OSPFv2

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

**SUMMARY STEPS**

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> show ip ospf [process-id] traffic [interface-type interface-number]</td>
<td>Displays OSPFv2 traffic statistics.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# show ip ospf traffic statistics</td>
<td></td>
</tr>
</tbody>
</table>
Displaying and Clearing OSPF Traffic Statistics for OSPFv3

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

SUMMARY STEPS

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show ipv6 ospf traffic statistics</td>
<td></td>
</tr>
<tr>
<td>Step 3 clear ipv6 ospf traffic</td>
<td>Clears OSPFv3 traffic statistics.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# clear ipv6 ospf traffic</td>
<td></td>
</tr>
</tbody>
</table>

Configuration Examples for OSPF Enhanced Traffic Commands
Displaying and Clearing Enhanced Traffic Statistics for OSPFv2 Example

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

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>11</td>
<td>528</td>
</tr>
<tr>
<td>RX DB des</td>
<td>4</td>
<td>148</td>
</tr>
<tr>
<td>RX LS req</td>
<td>1</td>
<td>60</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>3</td>
<td>216</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>RX Total</td>
<td>21</td>
<td>1080</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>14</td>
<td>1104</td>
</tr>
<tr>
<td>TX DB des</td>
<td>3</td>
<td>252</td>
</tr>
<tr>
<td>TX LS req</td>
<td>1</td>
<td>56</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>3</td>
<td>392</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>TX Total</td>
<td>23</td>
<td>1932</td>
</tr>
</tbody>
</table>

OSPF header errors:
- Length 0, Checksum 0, Version 0, Bad Source 0,
- No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
- Self Originated 0, Duplicate ID 0, Hello 0,
- MTU Mismatch 0, Nbr Ignored 0, LLS 0,
- Authentication 0,

OSPF LSA errors:
- Type 0, Length 0, Data 0, Checksum 0,

Interface Ethernet0/0

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>13</td>
<td>620</td>
</tr>
<tr>
<td>RX DB des</td>
<td>3</td>
<td>116</td>
</tr>
<tr>
<td>RX LS req</td>
<td>1</td>
<td>36</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>3</td>
<td>228</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>4</td>
<td>216</td>
</tr>
<tr>
<td>RX Total</td>
<td>24</td>
<td>1216</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>17</td>
<td>1344</td>
</tr>
<tr>
<td>TX DB des</td>
<td>4</td>
<td>276</td>
</tr>
<tr>
<td>TX LS req</td>
<td>1</td>
<td>56</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>7</td>
<td>656</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>2</td>
<td>128</td>
</tr>
<tr>
<td>TX Total</td>
<td>31</td>
<td>2460</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>24</td>
<td>1148</td>
</tr>
<tr>
<td>RX DB des</td>
<td>7</td>
<td>264</td>
</tr>
<tr>
<td>RX LS req</td>
<td>2</td>
<td>96</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>6</td>
<td>444</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>6</td>
<td>344</td>
</tr>
<tr>
<td>RX Total</td>
<td>45</td>
<td>2296</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>31</td>
<td>2448</td>
</tr>
<tr>
<td>TX DB des</td>
<td>7</td>
<td>528</td>
</tr>
<tr>
<td>TX LS req</td>
<td>2</td>
<td>112</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>10</td>
<td>1048</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>4</td>
<td>256</td>
</tr>
</tbody>
</table>
TX Total 54 4392
OSPF header errors
Length 0, Checksum 0, Version 0, Bad Source 13,
No Virtual Link 0, Area Mismatch 0, No Sham Link 0,
Self Originated 0, Duplicate ID 0, Hello 0,
MTU Mismatch 0, Nbr Ignored 0, LLS 0,
Authentication 0,
OSPF LSA errors
Type 0, Length 0, Data 0, Checksum 0,

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

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

Displaying and Clearing Enhanced Traffic Statistics for OSPFv3 Example

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

```
Router# show ipv6 ospf traffic

OSPFv3 statistics:
Rcvd: 32 total, 0 checksum errors
   10 hello, 7 database desc, 2 link state req
   9 link state updates, 4 link state acks
   0 LSA ignored
Sent: 45 total, 0 failed
   17 hello, 12 database desc, 2 link state req
   8 link state updates, 6 link state acks
OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
   Hello queue size 0, no limit, max size 2
   Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
   Interface Serial2/0
OSPFv3 packets received/sent
   Type          Packets              Bytes
   RX Invalid    0                    0
   RX Hello      5                    196
   RX DB des     4                    172
   RX LS req     1                    52
   RX LS upd     4                    320
   RX LS ack     2                    112
   RX Total      16                   852
   TX Failed     0                    0
   TX Hello      8                    304
   TX DB des     3                    144
   TX LS req     1                    52
   TX LS upd     3                    252
   TX LS ack     3                    148
   TX Total      18                   900
OSPFv3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,
Interface Ethernet0/0
OSPFv3 packets received/sent
   Type          Packets              Bytes
   RX Invalid    0                    0
   RX Hello      6                    240
   RX DB des     3                    144
   RX LS req     1                    52
   RX LS upd     5                    372
   RX LS ack     2                    152
   RX Total      17                   960
   TX Failed     0                    0
   TX Hello      11                   420
```
TX DB des  9  312
TX LS req  1  52
TX LS upd  5  376
TX LS ack  3  148
TX Total  29  1308

OSPFv3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,

OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,

Summary traffic statistics for process ID 6:

OSPFv3 packets received/sent
<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>11</td>
<td>436</td>
</tr>
<tr>
<td>RX DB des</td>
<td>7</td>
<td>316</td>
</tr>
<tr>
<td>RX LS req</td>
<td>2</td>
<td>104</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>9</td>
<td>692</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>4</td>
<td>264</td>
</tr>
<tr>
<td>RX Total</td>
<td>33</td>
<td>1812</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>19</td>
<td>724</td>
</tr>
<tr>
<td>TX DB des</td>
<td>12</td>
<td>456</td>
</tr>
<tr>
<td>TX LS req</td>
<td>2</td>
<td>104</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>8</td>
<td>628</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>6</td>
<td>296</td>
</tr>
<tr>
<td>TX Total</td>
<td>47</td>
<td>2208</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
<tr>
<td>OSPF configuration</td>
<td>Configuring OSPF</td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>
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 14 Feature Information for OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Enhanced Traffic Statistics for OSPFv2 and OSPFv3</td>
<td>12.4(6)T 12.2(31)SB2</td>
<td>This document describes the detailed OSPF traffic statistics that are provided when the user enters the new and modified commands show commands for OSPFv2 and OSPFv3. The following commands were introduced or modified: <code>clear ipv6 ospf traffic</code>, <code>show ip ospf traffic</code>, <code>show ipv6 ospf traffic</code>.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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 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, page 189
- Prerequisites for OSPF MIB Support of RFC 1850 and Latest Extensions, page 189
- Restrictions for OSPF MIB Support of RFC 1850 and Latest Extensions, page 190
- Information About OSPF MIB Support of RFC 1850 and Latest Extensions, page 190
- How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, page 195
- Configuration Examples for OSPF MIB Support of RFC 1850 and Latest Extensions, page 200
- Where to Go Next, page 200
- Additional References, page 200
- Feature Information for OSPF MIB Support of RFC 1850 and Latest Extensions, page 201

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.
Restrictions for OSPF MIB Support of RFC 1850 and Latest Extensions

For routers that are running Cisco IOS Release 12.0(26)S, 12.2(25)S, 12.2(27)/SBC, 12.2(31)/SB2 and later releases, the OSPF MIB and CISCO OSPF MIB will be supported only for the first OSPF process (except for MIB objects that are related to virtual links and sham links, and in cases where support for multiple topologies is provided). SNMP traps will be generated for OSPF events that are related to any of the OSPF processes. There is no workaround for this situation.

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, page 190
- Benefits of the OSPF MIB, page 194

OSPF MIB Changes to Support RFC 1850

- OSPF MIB, page 190
- OSPF TRAP MIB, page 191
- CISCO OSPF MIB, page 192
- CISCO OSPF TRAP MIB, page 193

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>
<thead>
<tr>
<th>OSPF-MIB Table</th>
<th>New MIB Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>OspfAreaEntry table</td>
<td>• OspfAreaSummary</td>
</tr>
<tr>
<td></td>
<td>• OspfAreaStatus</td>
</tr>
</tbody>
</table>
### OSPF-MIB Table

<table>
<thead>
<tr>
<th>New MIB Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>OspfStubAreaEntry • OspfStubMetricType</td>
</tr>
<tr>
<td>OspfAreaRangeEntry • OspfAreaRangeEffect</td>
</tr>
<tr>
<td>OspfHostEntry • OspfHostAreaID</td>
</tr>
<tr>
<td>OspfIfEntry • OspfIfStatus • OspfIfMulticastForwarding • OspfIfDemand • OspfIfAuthType</td>
</tr>
<tr>
<td>OspfVirtIfEntry • OspfVirtIfAuthType</td>
</tr>
<tr>
<td>OspfNbrEntry • OspfNbrmaNbrPermanence • OspfNbrHelloSuppressed</td>
</tr>
<tr>
<td>OspfVirtNbrEntry • OspfVirtNbrHelloSuppressed</td>
</tr>
<tr>
<td>OspfExtLsdbEntry • OspfExtLsdbType • OspfExtLsdbLsid • OspfExtLsdbRouterId • OspfExtLsdbSequence • OspfExtLsdbAge • OspfExtLsdbChecksum • OspfExtLsdbAdvertisement</td>
</tr>
<tr>
<td>OspfAreaAggregateEntry • OspfAreaAggregateAreaID • OspfAreaAggregateLsdbType • OspfAreaAggregateNet • OspfAreaAggregateMask • OspfAreaAggregateStatusospfSetTrap • OspfAreaAggregateEffect</td>
</tr>
</tbody>
</table>

---

**OSPF TRAP MIB**

This section describes scalar objects and MIB objects that are provided to support FRC 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 195.

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

### Table 16 New OSPF-TRAP-MIB Objects

<table>
<thead>
<tr>
<th>OSPF Control MIB Object</th>
<th>Trap MIB Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfSetTrap</td>
<td>• ospfIfStateChange</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtIfStateChange</td>
</tr>
<tr>
<td></td>
<td>• ospfNbrStateChange</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtNbrState</td>
</tr>
<tr>
<td></td>
<td>• ospfIfConfigError</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtIfConfigError</td>
</tr>
<tr>
<td></td>
<td>• ospfIfAuthFailure</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtIfAuthFailure</td>
</tr>
<tr>
<td></td>
<td>• ospfIfRxBadPacket</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtIfRxBadPacket</td>
</tr>
<tr>
<td></td>
<td>• ospfTxRetransmit</td>
</tr>
<tr>
<td></td>
<td>• ospfVirtIfTxRetransmit</td>
</tr>
<tr>
<td></td>
<td>• ospfOriginatelsa</td>
</tr>
<tr>
<td></td>
<td>• ospfMaxAgeLsa</td>
</tr>
</tbody>
</table>

### 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 CISCO-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 17  New CISCO-OSPF-MIB Objects

<table>
<thead>
<tr>
<th>CISCO-OSPF-MIB Table</th>
<th>New MIB Objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>cospfAreaEntry</td>
<td>• cospfOpaqueAreaLsaCount</td>
</tr>
<tr>
<td></td>
<td>• cospfOpaqueAreaLsaChecksum</td>
</tr>
<tr>
<td></td>
<td>• cospfAreaNssaTranslatorRole</td>
</tr>
<tr>
<td></td>
<td>• cospfAreaNssaTranslatorState</td>
</tr>
<tr>
<td></td>
<td>• cospfAreaNssaTranslatorEvents</td>
</tr>
<tr>
<td>cospfLsdbEntry</td>
<td>• cospfLsdbType</td>
</tr>
<tr>
<td></td>
<td>• cospfLsdbSequence</td>
</tr>
<tr>
<td></td>
<td>• cospfLsdbAge</td>
</tr>
<tr>
<td></td>
<td>• cospfLsdbChecksum</td>
</tr>
<tr>
<td></td>
<td>• cospfLsdbAdvertisement</td>
</tr>
<tr>
<td>cospfIfEntry</td>
<td>• cospfIfLsaCount</td>
</tr>
<tr>
<td></td>
<td>• cospfIfLsaChecksum</td>
</tr>
<tr>
<td>cospfVirtIfEntry</td>
<td>• cospfVirtIfLsaCount</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtIfLsaChecksum</td>
</tr>
<tr>
<td>cospfLocalLsdbEntry</td>
<td>• cospfLocalLsdbIpAddress</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbAddressLessIf</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbType</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbLsid</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbRouterId</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbAge</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbChecksum</td>
</tr>
<tr>
<td></td>
<td>• cospfLocalLsdbAdvertisement</td>
</tr>
<tr>
<td>cospfVirtLocalLsdbEntry</td>
<td>• cospfVirtLocalLsdbTransitArea</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbNeighbor</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbType</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbLsid</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbRouterId</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbSequence</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbAge</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbChecksum</td>
</tr>
<tr>
<td></td>
<td>• cospfVirtLocalLsdbAdvertisement</td>
</tr>
</tbody>
</table>

### CISCO OSPF TRAP MIB

The cospfSetTrapMIB 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-OSPFTRAP-MIB:

<table>
<thead>
<tr>
<th>CISCO-OSPF-TRAP-MIB Trap Events</th>
<th>Trap Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cospfIfConfigError</td>
<td>This trap is generated for mismatched MTU parameter errors that occur when nonvirtual OSPF neighbors are forming adjacencies.</td>
</tr>
<tr>
<td>cospfVirtIfConfigError</td>
<td>This trap is generated for mismatched MTU parameter errors when virtual OSPF neighbors are forming adjacencies.</td>
</tr>
<tr>
<td>cospfTxRetransmit</td>
<td>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.</td>
</tr>
<tr>
<td>cospfVirtIfTxRetransmit</td>
<td>This trap is generated in the case of opaque LSAs when packets are sent by a virtual interface.</td>
</tr>
<tr>
<td>cospfOriginateLsa</td>
<td>This trap is generated when a new opaque LSA is originated by the router when a topology change has occurred.</td>
</tr>
<tr>
<td>cospfMaxAgeLsa</td>
<td>The trap is generated in the case of opaque LSAs.</td>
</tr>
<tr>
<td>cospfNssaTranslatorStatusChange</td>
<td>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.</td>
</tr>
</tbody>
</table>

For information about how to enable OSPF MIB traps, see the How to Enable OSPF MIB Support of RFC 1850 and Latest Extensions, page 195.

**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, page 195
- Enabling Specific OSPF Traps, page 197
- Verifying OSPF MIB Traps on the Router, page 199

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server community <code>string1</code> ro</td>
<td>Enables read access to all objects in the MIB, but does not allow access to the community strings.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Routert(config)# snmp-server community public ro</td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server community <code>string2</code> rw</td>
<td>Enables read and write access to all objects in the MIB, but does not allow access to the community strings.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Routert(config)# snmp-server community private rw</td>
</tr>
<tr>
<td><strong>Step 5</strong> snmp-server host <code>hostname</code></td>
<td>Specifies a recipient (target host) for SNMP notification operations.</td>
</tr>
<tr>
<td>(ip-address)</td>
<td>• If no <code>notification-type</code> is specified, all enabled notifications (traps or informs) will be sent to the specified host.</td>
</tr>
<tr>
<td>[vrf vrf-name]</td>
<td>• If you want to send only the OSPF notifications to the specified host, you can use the optional <code>ospf</code> keyword as one of the <code>notification-types</code>. (See the example.) Entering the <code>ospf</code> keyword enables the ospfSetTrap trap control MIB object.</td>
</tr>
<tr>
<td>[traps</td>
<td></td>
</tr>
<tr>
<td>informs]</td>
<td></td>
</tr>
<tr>
<td>[version</td>
<td></td>
</tr>
<tr>
<td><code>1</code></td>
<td></td>
</tr>
<tr>
<td><code>2c</code></td>
<td></td>
</tr>
<tr>
<td><code>3</code></td>
<td></td>
</tr>
<tr>
<td>[auth</td>
<td></td>
</tr>
<tr>
<td>noauth</td>
<td></td>
</tr>
<tr>
<td>priv]</td>
<td></td>
</tr>
<tr>
<td>[community-string</td>
<td></td>
</tr>
<tr>
<td>udp-port</td>
<td></td>
</tr>
<tr>
<td>port]</td>
<td></td>
</tr>
<tr>
<td>[notification-type]</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Routert(config)# snmp-server host 172.20.2.162 version 2c public ospf</td>
</tr>
<tr>
<td><strong>Step 6</strong> snmp-server enable traps ospf</td>
<td>Enables all SNMP notifications defined in the OSPF MIBs.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Routert(config)# snmp-server enable traps ospf</td>
</tr>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Ends your configuration session and exits global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Routert(config)# end</td>
</tr>
</tbody>
</table>

**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 type 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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> snmp-server enable traps ospf cisco-specific errors [config-error] [virt-config-error]</td>
<td>Enables SNMP notifications for Cisco-specific OSPF configuration mismatch errors.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• Entering the <code>snmp-server enable traps ospf cisco-specific errors</code> command with the optional <code>virt-config-error</code> keyword enables only the SNMP notifications for configuration mismatch errors on virtual interfaces.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# snmp-server enable traps ospf cisco-specific errors config-error</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong> snmp-server enable traps ospf cisco-specific</td>
<td>Enables error traps for Cisco-specific OSPF errors that involve re-sent packets.</td>
</tr>
<tr>
<td>retransmit [packets] [virt-packets]</td>
<td>• Entering the <code>snmp-server enable traps ospf cisco-specific retransmit</code> command with the optional <code>virt-packets</code> keyword enables only the SNMP notifications for packets that are re-sent on virtual interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>cisco-specific retransmit packets virt-packets</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> snmp-server enable traps ospf cisco-specific</td>
<td>Enables all error traps for Cisco-specific OSPF transition state changes.</td>
</tr>
<tr>
<td>state-change [nssa-trans-change] [shamlink-state-change]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>cisco-specific state-change</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> snmp-server enable traps ospf cisco-specific</td>
<td>Enables error traps for opaque LSAs.</td>
</tr>
<tr>
<td>lsa [lsa-maxage] [lsa-originate]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>cisco-specific lsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> snmp-server enable traps ospf errors</td>
<td>Enables error traps for OSPF configuration errors.</td>
</tr>
<tr>
<td>authentication-failure [bad-packet] [config-error] [</td>
<td>• Entering the <code>snmp-server enable traps ospf errors</code> command with the optional <code>virt-config-error</code> keyword enables only the SNMP notifications for OSPF configuration errors on virtual interfaces.</td>
</tr>
<tr>
<td>virt-authentication-failure] [virt-config-error]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>errors virt-config-error</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> snmp-server enable traps ospf lsa</td>
<td>Enables error traps for OSPF LSA errors.</td>
</tr>
<tr>
<td>lsa-maxage [lsa-originate]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>lsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> snmp-server enable traps ospf rate-limit</td>
<td>Sets the rate limit for how many SNMP OSPF notifications are sent in each OSPF SNMP notification rate-limit window.</td>
</tr>
<tr>
<td>seconds trap-number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# snmp-server enable traps ospf</td>
<td></td>
</tr>
<tr>
<td>rate-limit 20 20</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

#### Step 10
snmp-server enable traps ospf retransmit [packets] [virt-packets]

**Purpose:** Enables SNMP OSPF notifications for re-sent packets.

**Example:**
```
Router(config)# snmp-server enable traps ospf retransmit
```

#### Step 11
snmp-server enable traps ospf state-change [if-state-change] [neighbor-state-change] [virtif-state-change] [virtneighbor-state-change]

**Purpose:** Enables SNMP OSPF notifications for OSPF transition state changes.

**Example:**
```
Router(config)# snmp-server enable traps ospf state-change
```

## Verifying OSPF MIB Traps on the Router

### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** show running-config [options] | Displays the contents of the currently running configuration file and includes information about enabled traps. |
| **Example:** | Verifies which traps are enabled. |
| Router# show running-config | include traps |

---

**Example:**
```
Router(config)# snmp-server enable traps ospf state-change
```
Configuration Examples for OSPF MIB Support of RFC 1850 and Latest Extensions

- Example Enabling and Verifying OSPF MIB Support Traps, page 200

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 Configuration Fundamentals and Network Management Configuration Guide, Release 12.2.

Additional References

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

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP commands</td>
<td>Cisco IOS Configuration Fundamentals and Network Management Command Reference</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
**MIB**

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-OSPF-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
<tr>
<td>• CISCO-OSPF-TRAP-MIB</td>
<td></td>
</tr>
<tr>
<td>• OSPF-MIB</td>
<td></td>
</tr>
<tr>
<td>• OSPF-TRAP-MIB</td>
<td></td>
</tr>
</tbody>
</table>

**RFC**

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 1850</td>
<td>OSPF MIB Support</td>
</tr>
</tbody>
</table>

**Technical Assistance**

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

---

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF MIB Support of RFC 1850 and Latest Extensions</td>
<td>12.0(26)S 12.3(4)T 12.2(25)S 12.2(27)SBC 12.2(31)SB2</td>
<td>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.</td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.
SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields

This document describes the configuration command that allows you to use either the current interface number or the SNMP MIB-II interface index (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.

• Finding Feature Information, page 203
• Prerequisites for Interface ID in Data Fields, page 203
• Information About Interface ID in Data Fields, page 203
• How to Configure the Interface ID in Data Fields, page 204
• Configuration Examples for the Interface ID in Data Fields, page 206
• Additional References, page 210
• Feature Information for SNMP ifIndex Value for Interface ID in Data Fields, page 211
• Glossary, page 211

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 Interface ID in Data Fields

OSPF must be configured on the router.

Information About Interface ID in Data Fields

Before choosing to switch from the current interface numbers to the SNMP MIB-II interface ID numbers, you should understand the following concepts:

• Benefits of Choosing to Identify Interfaces by the SNMP MIB-II ifIndex Value, page 204
• How OSPFv2 and OSPFv3 Use the SNMP MIB-II ifIndex Value, page 204
Benefits of Choosing to Identify Interfaces by the SNMP MIB-II ifIndex Value

If you use Simple Network Management Protocol (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 (interface index) 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.
- When examining 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.
- When looking at the output of 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 the Interface ID in Data Fields

- Using SNMP MIB-II ifIndex Numbers, page 204

Using SNMP MIB-II ifIndex Numbers

Follow the steps in this task to configure OSPF interfaces to use the SNMP MIB-II ifIndex numbers. These steps work for both OSPFv2 and OSPFv3. All OSPF interfaces must use the SNMP MIB-II ifIndex
numbers or the interfaces will not be enabled for OSPF. Therefore, repeat the steps within this task for each OSPF process for which you want the interfaces to use the 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** [interface-type] [slot /][port-adapter /][port]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2 configure terminal**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3** Do one of the following:

- `router ospf process-id [vrf vpn-name]`
- `ipv6 router ospf process-id`

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Configures an OSPFv2 routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Router(config)# router ospf 4</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Configures an OSPFv3 routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Router(config)# ipv6 router ospf 4</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose
--- | ---
**Step 4** interface-id snmp-if-index | Configures OSPF interfaces with the SNMP interface index identification numbers (ifIndex values).

**Example:**
```
Router(config-router)# interface-id snmp-if-index
```

**Step 5** `end` | Returns to privileged EXEC mode.

**Example:**
```
Router(config-router)# end
```

**Step 6** `show snmp mib ifmib ifindex [interface-type] [slot ][port-adapter /][port]` | Displays SNMP interface index identification numbers (ifIndex values) for all the system interfaces or the specified system interface.

**Example:**
```
Router# show snmp mib ifmib ifindex Ethernet 0/1
```

---

### Configuration Examples for the Interface ID in Data Fields

- Configuring the SNMP ifIndex Value for Interface ID for OSPFv2 Example, page 206
- Configuring the SNMP ifIndex Value for Interface ID for OSPFv3 Example, page 207

### Configuring the SNMP ifIndex Value for Interface ID for OSPFv2 Example

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 iIfIndex 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)# *
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
```
Configuring the SNMP ifIndex Value for Interface ID for OSPFv3 Example

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 OSPFv3 data fields.

Router# show snmp mib ifmib ifindex Ethernet1/0
Ethernet1/0: Ifindex = 5
Router# show ipv6 ospf int
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 0 neighbor(s)
Ethernet2/0 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
  Transmmit 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)
Ethernet1/0 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 data net adv 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 data prefix adv 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: 2002:0:1::
    Prefix Length: 64, Options: None, 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 data 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 data link adv 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: Ethernet2/0)
Link State ID: 10 (Interface ID)
Advertising Router: 172.16.0.1
LS Seq Number: 80000002
Checksum: 0xA9CB
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: Ethernet1/0)
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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td>Cisco IOS IP Routing: OPSF Command Reference</td>
</tr>
<tr>
<td>OSPF configuration</td>
<td>&quot;Configuring OSPF&quot;</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2328</td>
<td>OSPF Version 2</td>
</tr>
<tr>
<td>RFC 2740</td>
<td>OSPF Version 3</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for SNMP ifIndex Value for Interface ID in Data Fields

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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF: SNMP ifIndex Value for Interface ID in OSPFv2 and OSPFv3 Data Fields</td>
<td>12.4(6)T 12.2(31)SB2 12.2(33)SRB</td>
<td>This document describes the configuration command that allows you the choice to use 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.</td>
</tr>
</tbody>
</table>

Glossary

SNMP --Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite.
Note

See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.
This document focuses on nonstop forwarding (NSF) for OSPFv2 in Cisco IOS software, using the IETF standardized graceful restart functionality that is described in RFC 3623. Under very specific situations, a router may undergo certain well-known failure conditions that should not affect packet forwarding across the switching platform. NSF capability allows for the forwarding of data packets to continue along routes that are already known, while the routing protocol information is being restored. This capability is useful in cases in which there is a component failure (for example, a Route Processor [RP] crash with a backup RP taking over) or in which there is a scheduled hitless software upgrade.

Prior to RFC 3623, Cisco implemented Cisco-proprietary NSF, referred to as Cisco NSF. The OSPF RFC 3623 Graceful Restart feature allows you to configure IETF NSF in multivendor networks. Configuring IETF NSF increases the availability of your network by allowing OSPF routers to stay on the forwarding path even as their OSPF software is restarted. This document refers to the two forms of NSF as Cisco NSF and IETF NSF. The OSPF RFC 3623 Graceful Restart feature is the latest addition to the Cisco High Availability portfolio.

- Finding Feature Information, page 213
- Prerequisites for Configuring IETF NSF or Cisco NSF, page 213
- Restrictions for Configuring IETF NSF or Cisco NSF, page 214
- Information About IETF NSF and Cisco NSF, page 214
- How to Configure IETF NSF or Cisco NSF, page 217
- Configuration Examples for IETF NSF or Cisco NSF, page 220
- Additional References, page 221
- Feature Information for NSF-OSPF RFC 3623 Graceful Restart, page 222
- Glossary, page 223

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 Configuring IETF NSF or Cisco NSF
Restrictions for Configuring IETF NSF or Cisco NSF

- Only one of the possible methods for nonstop forwarding (Cisco NSF or IETF NSF) is supported at a time. For example, the restarting router uses either Cisco NSF or IETF NSF during switchover, depending on the configuration of the router. The helper mode for both methods is supported by default, based on the restarting method used by the restarting router. For example, if the restarting router is IETF NSF-capable, the helper router will use IETF NSF helper mode by default.
- Neither Cisco NSF nor IETF NSF is supported over sham-links.
- Cisco NSF is not support over virtual links.

Information About IETF NSF and Cisco NSF

- Cisco NSF Routing and Forwarding Operation, page 214
- Cisco Express Forwarding for NSF, page 214
- OSPF Graceful Restart Functionality per RFC 3623, page 215

Cisco NSF Routing and Forwarding Operation

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

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

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

Cisco Express Forwarding for NSF

A key element of NSF is packet forwarding. The OSPF protocol depends on CEF to continue forwarding packets during switchover while the routing protocols rebuild the Routing Information Base (RIB) tables. Once OSPF has converged, CEF updates the Forwarding Information Base (FIB) table and removes stale route entries. CEF then updates the line cards with the new FIB information. CEF maintains the FIB and uses the FIB information that was current at the time of a switchover to continue forwarding packets during the switchover. This feature reduces traffic interruption during the switchover.
During normal NSF operation, CEF on the active RP synchronizes its current FIB and adjacency databases with the FIB and adjacency databases on the standby RP. Upon switchover of the active RP, the standby RP initially has FIB and adjacency databases that are mirror images of those that were current on the active RP. For platforms with intelligent line cards, the line cards maintain the current forwarding information over a switchover; for platforms with forwarding engines, CEF keeps the forwarding engine on the standby RP current with changes that are sent to it by CEF on the active RP. In this way, the line cards or forwarding engines can continue forwarding after a switchover as soon as the interfaces and a data path are available.

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

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

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

---

**OSPF Graceful Restart Functionality per RFC 3623**

This section describes the RFC 3623 graceful restart nonstop forwarding enhancement to the OSPF routing protocol. An OSPF NSF-capable router that is reloading and attempting a graceful restart originates grace- lsas to notify its neighbors that it will perform graceful restart within the specified amount of time or grace period. During this grace period, the neighboring OSPF routers, called helper routers, continue to announce the restarting router in their LSAs as if it were fully adjacent, as long as the network topology remains static.

The following sections contain more detailed information about the graceful restart process:

- [Graceful Restart Router Operation](#), page 215
- [Graceful Restart Helper Mode Operation](#), page 216

**Graceful Restart Router Operation**

**Graceful Restart Initiation**

The restarting router becomes aware that it should start the graceful restart process when the network administrator issues the appropriate command or when an RP reloads and forces and Redundancy Facility (RF) switchover. The length of the grace period can be set by the network administrator or calculated by the OSPF software of the restarting router. In order to prevent the LSAs from the restarting router from aging out, the grace period should not exceed an LSA refresh time of 1800 seconds.

In preparation for graceful restart, the restarting router must perform the following action before its software can be reloaded: The restarting router must ensure that its forwarding table is updated and will
remain in place during the restart. No OSPF shutdown procedures are performed since neighbor routers must act as if the restarting router is still in service.

The OSPF software is reloaded on the router (it undergoes graceful restart).

**OSPF Processes During Graceful Restart**

After the router has reloaded, it must modify its OSPF processes until it reestablishes full adjacencies with all former fully adjacent OSPF neighbors. During graceful restart, the restarting router modifies its OSPF processes in the following ways:

- The restarting router does not originate LSAs with LS types 1, 5, or 7 so that the other routers in the OSPF domain will use the LSAs that the restarting router had originated prior to reloading. The router does not modify or flush any self-originated LSAs.
- The restarting router runs its OSPF routing calculations in order to return any OSPF virtual links to operation. However, the restarting router does not install OSPF routes into the system’s forwarding table, and the router relies on the forwarding entries that it had installed prior to undergoing the graceful restart process.
- If the restarting router determines that it was the Designated Router on a given segment prior to the graceful restart, it will reelect itself.

**Graceful Restart Process Exit**

The restarting router exits the graceful restart process when one of the following events occur:

- The router has reestablished all adjacencies. The graceful restart was successful.
- The router receives an LSA that is inconsistent with an LSA from the same router prior to the graceful restart. The inconsistency can be mean either that the router does not support the graceful restart feature or that the router has terminated its helper mode for some reason. The graceful restart was unsuccessful.
- The grace period has expired. The graceful restart was not successful.
- Once the restarting router has completed the graceful restart process, it returns to normal OSPF operation, reoriginating LSAs based on the current state of the router and updating its forwarding tables based on current link-state database contents. At this time, it flushes the grace-lsas that it had originated during the initiation of the graceful restart process.

**Graceful Restart Helper Mode Operation**

**Helper Mode Initiation**

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

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

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

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

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

How to Configure IETF NSF or Cisco NSF

- Enabling IETF NSF or Cisco NSF on the Router, page 217
- Enabling Graceful Restart Strict LSA Checking on a Helper Router, page 218

Enabling IETF NSF or Cisco NSF on the Router

Complete the steps in the following task to configure and verify configuration of Cisco NSF or IETF NSF on the router.

In order for the graceful restart process to work successfully, the OSPF neighbor (helper) routers need to run a version of Cisco IOS software that supports Cisco NSF or IETF NSF, or both.

SUMMARY STEPS

1. enable
2. configure terminal
3. router ospf process-id [vrf vpn-name]
4. nsf ietf [restart-interval seconds]
5. end
6. show ip ospf [process-id]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

Example:

Router> enable

Router>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
| **Example:** 

Router# configure terminal | |
| **Step 3** router ospf *process-id* [vrf *vpn-name*] | Configures an Open Shortest Path First (OSPF) routing process and enters router configuration mode. |
| **Example:** 

Router(config)# router ospf 4 | |
| **Step 4** nsf ietf [restart-interval *seconds*] | (Optional) Enables IETF NSF, or graceful restart, on the router. |
| **Example:** 

nsf cisco [enforce global] | - Optionally configures a maximum graceful restart interval, in seconds, after the graceful restart process. or 
| **Example:** 

Router(config-router)# nsf ietf restart-interval 600 | (Optional) Enables Cisco NSF on a Cisco router. |
| **Example:** 

Router(config-router)# nsf cisco | |
| **Step 5** end | Returns to privileged EXEC mode. |
| **Example:** 

Router(config-router)# end | |
| **Step 6** show ip ospf [process-id] | Displays general information about OSPF routing processes and whether OSPF graceful restart is configured. |
| **Example:** 

Router# show ip ospf 4 | |

**Enabling Graceful Restart Strict LSA Checking on a Helper Router**

Graceful restart helper mode is enabled by default. It is not recommended to disable helper mode because the disabled neighbor will detect the lost adjacency and the graceful restart process will be terminated.
The strict LSA checking feature allows a helper router to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. Strict LSA checking is disabled by default. You can enable strict LSA checking on an OSPF helper to have the router terminate graceful restart when there is a change to an LSA that would be flooded to the restarting router. You can configure strict LSA checking on both NSF-aware and NSF-capable routers; however, this feature will become effective only when the router is in helper mode.

Complete the steps in the following task to disable helper mode or enable strict LSA checking on the NSF-aware (helper) router.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. router ospf process-id [vrf vpn-name]
4. nsf cisco helper disable
5. nsf ietf helper strict-lsa-checking
6. end
7. show ip ospf [process-id]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 router ospf process-id [vrf vpn-name]</td>
<td>Configures an Open Shortest Path First (OSPF) routing process and enters router configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
</tbody>
</table>

Example:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 454
```
### Command or Action | Purpose
--- | ---
**Step 4**
nsf cisco helper disable | (Optional) Disables helper mode for Cisco NSF. or (Optional) Disables helper mode for IETF NSF.  
--- | ---
Example:  
nsf ietf helper disable |  
--- | ---
Example:  
Router(config-router)# nsf cisco helper disable  
--- | ---
Example:  
Router(config-router)# nsf ietf helper disable |  
--- | ---
**Step 5**
nsf ietf helper strict-lsa-checking | Enables strict LSA checking on an NSF-aware (helper) router.  
--- | ---
Example:  
Router(config-router)# nsf ietf helper strict-lsa-checking |  
--- | ---
**Step 6**
end | Returns to privileged EXEC mode.  
--- | ---
Example:  
Router(config-router)# end |  
--- | ---
**Step 7**
show ip ospf [process-id] | Displays general information about OSPF routing processes and whether helper mode or strict LSA checking is enabled for the NSF-aware (helper) router.  
--- | ---
Example:  
Router# show ip ospf 454 |  
--- | ---

### Configuration Examples for IETF NSF or Cisco NSF
- Enabling and Verifying IETF NSF for OSPF Example, page 221
- Disabling Helper Mode for IETF NSF Example, page 221
Enabling and Verifying IETF NSF for OSPF Example

The following example enables IETF NSF for OSPF process 10 on the router. The restart interval has been changed from the 120-second default value to 200 seconds.

Router(config)# router ospf 10
Router(config-router)# nsf ietf restart-interval 200
Router(config-router)# end

When the `show ip ospf` command is entered for OSPF process 10, the output verifies that IETF NSF was configured on the router, with a maximum route lifetime interval set for 200 seconds. The command output also confirms that NSF helper mode is enabled by default for IETF NSF, as well as for Cisco NSF.

Router# show ip ospf 10
Routing Process "ospf 10" with ID 172.16.2.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 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
IETF Non-Stop Forwarding enabled
  restart-interval limit: 200 sec
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 4 (1 loopback)
  Area has no authentication
  SPF algorithm last executed 02:03:02.468 ago
  SPF algorithm executed 4 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x175DA
  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

Disabling Helper Mode for IETF NSF Example

The following configuration disables helper support for IETF NSF on an OSPF router.

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

Additional References

The following sections provide references related to the OSPF RFC 3623 Graceful Restart feature.
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
<tr>
<td>OSPF configuration</td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>Cisco nonstop forwarding</td>
<td>Cisco Nonstop Forwarding</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 2328</td>
<td><em>OSPF Version 2</em></td>
</tr>
<tr>
<td>RFC 3623</td>
<td><em>Graceful OSPF Restart</em></td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
<tr>
<td>documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</td>
<td></td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF--OSPF (RFC 3623 OSPF</td>
<td>12.0(32)S 12.2(33)SRA</td>
<td>This document focuses on nonstop forwarding (NSF) for OSPFv2 in Cisco IOS software,</td>
</tr>
<tr>
<td>Graceful Restart)</td>
<td>12.2(31)SB2 12.2(33)SXH</td>
<td>using the IETF standardized graceful restart functionality as described in RFC 3623.</td>
</tr>
</tbody>
</table>

Glossary

cutover -- An event in which system control and routing protocol execution are transferred from an active processor to a standby processor. This may include transfer of the packet forwarding function as well.

NSF -- nonstop forwarding. The continuation of forwarding packets across line cards during RP cutover.

OSPF -- Open Shortest Path First. An interior gateway routing protocol.

RF -- Redundancy Facility. A state machine that controls the progression and state of the redundant processor cards.

RP -- Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor.

switchover -- See cutover.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.
Area Command in Interface Mode for OSPFv2

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, page 225
- Prerequisites for Area Command in Interface Mode for OSPFv2, page 225
- Restrictions for Area Command in Interface Mode for OSPFv2, page 225
- Information About Area Command in Interface Mode for OSPFv2, page 226
- How to Enable the Area Command in Interface Mode for OSPFv2, page 227
- Configuration Examples for Area Command in Interface Mode for OSPFv2 Feature, page 228
- Additional References, page 229
- Feature Information for Area Command in Interface Mode for OSPFv2, page 230

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 Area Command in Interface Mode for OSPFv2

OSPFv2 must be running on your network.

Restrictions for Area Command in Interface Mode for OSPFv2

The `ip ospf area` command is supported only for OSPFv2.
Information About Area Command in Interface Mode for OSPFv2

Benefits of Area Command in Interface Mode for OSPFv2 Feature

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 that is entered in router configuration mode. You can enable OSPFv2 explicitly on an interface with the `ip ospf area` command that 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 will supersede the effects of the `network area` command that 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.

Configuration Guidelines for the Area Command in Interface Mode for OSPFv2 Feature

When you use the `ip ospf area` command in interface configuration mode to enable OSPFv2 on an interface, we recommend that you be familiar with the following guidelines.

**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 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 interface enable Command

When the interface enable 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 interface enable 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 the Area Command in Interface Mode for OSPFv2

- Enabling OSPFv2 on an Interface, page 227

Enabling OSPFv2 on an Interface

Perform this task to enable 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 [interface-type interface-number]
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  - Enter your password if prompted. |

  **Example:**
  
  ```
  Router> enable
  ```

| **Step 2** configure terminal | Enters global configuration mode. |

  **Example:**
  
  ```
  Router# configure terminal
  ```

| **Step 3** interface type number | Configures an interface type and enters interface configuration mode. |

  **Example:**
  
  ```
  Router(config)# interface FastEthernet 0/2
  ```

| **Step 4** ip ospf process-id area area-id [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. |

  **Example:**
  
  ```
  Router(config-if)# ip ospf 1 area 0 secondaries none
  ```

| **Step 5** end | Exits interface configuration mode and returns to privileged EXEC mode. |

  **Example:**
  
  ```
  Router(config-if)# end
  ```

| **Step 6** show ip ospf interface [interface-type interface-number] | 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. |

  **Example:**
  
  ```
  Router# show ip ospf interface FastEthernet 0/2
  ```

---

### Configuration Examples for Area Command in Interface Mode for OSPFv2 Feature

- Example: Enabling OSPFv2 on an Interface, page 229
Example: Enabling OSPFv2 on an Interface

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

```
Router(config)# interface Ethernet 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 Ethernet 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 Ethernet 0/0/0
Ethernet0/0/0 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
        Neighbors 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 the Area Command in Interface Mode for OSPFv2 feature.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF commands</td>
<td><em>Cisco IOS IP Routing: OSPF Command Reference</em></td>
</tr>
<tr>
<td>OSPF configuration tasks</td>
<td>&quot;Configuring OSPF&quot; module</td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td></td>
</tr>
</tbody>
</table>
MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

| RFC 2328 | OSPF Version 2 |

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for Area Command in Interface Mode for OSPFv2

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 Area Command in Interface Mode for OSPFv2

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Command in Interface Mode for OSPFv2</td>
<td>12.0(29)S</td>
<td>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 <strong>ip ospf area</strong> command allows you to enable OSPFv2 explicitly on an interface. The <strong>ip ospf area</strong> command is an alternative to enabling OSPFv2 through the address of the interface that matches the address range specified by the <strong>network area</strong> command.</td>
</tr>
<tr>
<td></td>
<td>12.3(11)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(28)SB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>15.0(1)SY</td>
<td></td>
</tr>
</tbody>
</table>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, 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.